TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MATIAS LEINONEN

LAYER 2 ETHERNET COMMUNICATION TUNNELING POSSIBILITIES IN AUTOMATION SYSTEMS

Master of Science thesis

Examiner: prof. Hannu Koivisto
Jari Seppälä
Examiner and topic approved by the Engineering Sciences Faculty Council meeting on 30th of August 2017

ABSTRACT

MATIAS LEINONEN: Layer 2 Ethernet Communication Tunneling Possibilities in Automation Systems
Tampere University of Technology
Master of Science Thesis, 53 pages, 1 Appendix pages
September 2017
Master's Degree Programme in Automation Technology
Major: Automation Software Engineering
Examiner: Professor Hannu Koivisto, Jari Seppälä
Keywords: layer 2, communication, Data Link Layer, Ethernet, tunneling, real-time

Future trends in energy generation are renewable energy sources and distributed energy generation. In control systems, these changes require higher automatization, more intelligent devices and secure and reliable communication. Another requirement is faster communication. Building a system that is able to fulfill real-time communication requirements over network layer is a hindrance to automation systems. There are multiple protocols that can manage the requirements, but many of them have limitations and requirements of their own. The limitations can be related to packet sizes, used devices or they may require a license. Tunneling protocols can bring a more general solution for the real-time problem. Tunneling Ethernet communication over network layer and letting the tunneling protocol to handle the network layer packaging instead of the communication protocol removes the need of a layer 3 protocol. Layer 2 tunneling provides a direct connection between separate local area networks. It enables a way for devices to communicate with each other over network layer using layer 2 communication protocols. Tunnel uses a pre-configured route to the destination gateway device making the routing of messages simpler and faster than with traditional IP routing. Layer 2 tunneling can be used in any communication system that utilizes layer 2 and layer 3 communication. This thesis focuses on use of tunneling in automation systems.

The purpose of this thesis is to provide information and possible solutions for layer 2 Ethernet tunneling. The main focus is in suitable tunneling protocols and communication protocols, but also security and resilience solutions are studied. This thesis is composed of published studies, researches, articles and books that address the topic.

TIIVISTELMÄ

MATIAS LEINONEN: Layer 2 ethernet-kommunikaation tunnelointimahdollisuudet automaatiojärjestelmissä
Tampereen teknillinen yliopisto
Diplomityö, 53 sivua, 1 liitesivua
Syyskuu 2017
Automaatiotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Automaation ohjelmistotekniikka
Tarkastaja: professori Hannu Koivisto, Jari Seppälä
Avainsanat: Layer 2, kommunikaatio, siirtoyhteyskerros, Ethernet, tunnelointi, reaaliaika

Tulevaisuuden trendit sähköntuotannossa ovat uusiutuvat energialähteet ja hajautettu energiantuotanto. Muutokset, joita nämä suuntaukset tuovat ohjausjärjestelmiin ovat korkeampi automaatio, älykkäiden laitteiden suurempi määrä sekä turvattu ja luotettava kommunikaatio. Näiden lisäksi vaaditaan nopeampaa tiedonsiirtoa. Järjestelmän rakentaminen, joka täyttää reaaliaikaisen kommunikaation asettamat vaatimukset verkkokerroksen yli on ongelmallinen automaatiojärjestelmille. Useita protokollia on kehitetty täyttämään reaaliaikavaatimukset, mutta niistä monissa on rajoituksia ja omia vaatimuksia järjestelmille. Rajoitukset voivat koskea pakettien kokoa, käytettyjä laitteita tai niiden käyttö voi vaatia lisenssiä. Tunnelointiprotokollat voivat tuoda yleispätevän ratkaisun reaaliaikaongelmaan. Tunneloimalla Ethernet-viestejä verkkokerroksen yli, ja antaa tunnelointiprotokollan hoitaa viestien paketointi, poistetaan tarve ylemmän tason kommunikointiprotokollalle. Layer 2-tunnelointi tarjoaa suoran yhteyden erillisten lähiverkkojen välille ja mahdollistaa lähiverkkojen laitteiden välisen kommunikaation verkkon yli käyttäen lähiverkkoprotokollia. Tunneli käyttää esikonfiguroitua reittiä pääteasemana toimivaan laitteeseen, joka nopeuttaa ja yksinkertaistaa viestien reitittämistä verrattuna perinteiseen IP-pakettien reititykseen. Layer 2-tunnelointia voidaan hyödyntää missä vain kommunikaatiojärjestelmässä, jossa käytetään layer 2- ja layer 3-kommunikaatiota. Tässä diplomityössä keskitytään tunneloinnin hyödyntämiseen automaatiojärjestemissä.

Työn tarkoituksena on tarjota tietoa ja mahdollisia ratkaisuja siirtoyhteyskerroksen ethernet kommunikaation tunnelointiin. Päätutkimuskohteina ovat sopivat tunnelointiprotokollat sekä kommunikointiprotokollat, mutta tutkittavia alueita ovat myös tietoturva ja vikasietoisuus. Työn sisältö on koostettu aihetta käsittelevistä julkaistuista, tutkimuksista, artikkeleista sekä kirjoista.

PREFACE

This Master's thesis was done for Tampere University of Technology the department of Automation Science and Engineering and it was written during 2016 and 2017. The topic of this thesis is related to a FLEXe program that the department is participating in. The FLEXe program is organized by CLIC Innovation and it researches flexible energy systems that can be used in the future. This thesis is written to people who are working with or interested in layer 2 communication, Ethernet solutions, automation systems or with electricity networks. I hope this study provides useful information about layer 2 tunneling possibilities.

I would like to thank my thesis supervisor and examiner professor Hannu Koivisto for his help and counsel during my writing process. I am also hugely grateful for Jari Seppälä, my other examiner, whose adept knowledge of the topic was a tremendous help. Now that I look back, I should have consulted with them more often. I also want to thank Mikko Salmenperä for his initial help and information which helped me to get the work started.

My deepest gratitude goes to my wife whose support did not falter even in the most difficult times. I also owe thanks to my family who supported me during this long project. Special thanks to my grandfather and his encouraging words.

Tampere, 13.08.2017

Matias Leinonen

CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

ACSI Abstract Communication Service Interface

ADU Application Data Unit

AH Authentication Header

ASDU Application Service Data Units

APDU Application Protocol Data Unit

BFD Bidirectional Forwarding Detection

CBA Component Based Automation

CE Customer Edge

CIP Common Industrial Protocol

CRC Cyclic Redundancy Check

CVC Coordinated Voltage Control

DCOM Distributed Component Object Model

DG Distributed Generation

DN Distribution Network

DNP3 Distributed Network Protocol 3

EoMPLS Ethernet over MPLS

ESP Encapsulating Security Payload

FLEXe Flexible Energy System

GOOSE Generic Object Oriented Substation Event

GRE Generic Routing Encapsulation

GSE Generic Substation Event

GSSE Generic Substation State Event

HSR High Availability Seamless Redundancy Protocol

IEC International Electrotechnical Commission

IED Intelligent Electronic Device

IGP Interior Gateway Protocol

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IO Input/Output

IOT Internet of Things

IP Inter-networking Protocol

IPSec IP Security

ISO International Organization for Standardization

L2TP Layer 2 Tunneling Protocol

L2TPv3 Layer 2 Tunneling Protocol version 3

LAC L2TP Access Concentrator

LAG Link Aggregation Group

LAN Local Area Network

LCCE L2TP Control Connection Endpoint

LDP Label Distribution Protocol

LLC Logical Link Control

LNS L2TP Network Server

LSR Label Switching Routers

LV Low Voltage

MAC Media Access Control

MACSec MAC Security

MAN Metropolitan-area Network

MC-LAG Multi-Chassis LAG

MD Message Digest

MMS Manufacturing Message Specification

MPDU MACSec Protocol Data Unit

MPLS Multiprotocol Label Switching

MV Medium Voltage

NCS Network Control System

OSI Open Systems Interconnection

OSPF Open Shortest Path First

PDU Protocol Data Unit

PE Provider Edge

PLC Power-line communication

PLC Programmable Control Unit

PRP Parallel Redundancy Protocol

PWE3 Pseudowire Emulation Edge-to-Edge

RTU Remote Terminal Unit

SCADA Supervisory Control and Data Acquisition

SHA Secure Hash Algorithm

SS Secondary substation

SV Sampled Values

TC 57 Technical Committee 57

TCP Transport Control Protocol

TUT Tampere University of Technology

UDP User Datagram Protocol

VCCV Virtual Circuit Connectivity Verification

VLAN Virtual Local Area Network

VPN Virtual Private Network

WAN Wide Area Network

WLAN Wireless Local Area Network

XML Extensible Markup Language

1. INTRODUCTION

1.1 Motivation

If we look at the growing trends in power engineering renewable energy sources and distributed energy generation are the directions we are moving towards. For control systems this means higher automatization, more intelligent devices and secure and reliable communication. One example where this can be seen is the growing popularity of smart grids, which is an intelligent power delivery network designed for providing two-way flow of electricity and information. Smart grids have been developed to improve the controllability and information sharing in distribution networks. Automation systems are the core of smart grid solutions. This means that the future improvements, concerning efficiency, safety and sustainability, of the energy supply are focused on automation systems [11].

Distributed generation (DG) means that energy generation is decentralized and the generators vary in size and type [1]. The energy produced with DG can be used by the generator owner or it can be provided into a distribution network (DN) grid. Typical technologies for DG are (solar) photovoltaic panels, wind turbines, combined heat and power installations and geothermal systems. Movement towards using DG and renewable energy sources is increasing due to the rising awareness of global warming and need to cut carbon dioxide emissions. Another reason DG is gaining popularity is that energy generation is possible for anyone and it no longer requires large factories and huge investments. Currently DG installations are mostly done by small commercial customers, communities and households, but also energy companies have started to invest in DG and started building their own distributed generators.

Smart grids and large-scale implementation of DG changes the distribution networks into a wider system where the requirements for communication are higher. Data like measurement values, state information and alarms needs to be transferred reliably, securely and most importantly fast. Today, providing hard or soft, real-time communication over a network layer is a huge problem. Pure Ethernet communication can fulfill the time requirements of real-time communication but only in local area networks (LAN). Multiple Ethernet protocols that can communicate over network layer have been created to solve this, but their performance level varies depending on the system. They use a layer 3 stack and map the Ethernet frames to network layer packets, for example IP packets. An alternative method that provides a solution for transferring Ethernet frames over network layer is tunneling and that is what this thesis studies.

1.2 Objective

The objective of this thesis is to provide information about the layer 2 Ethernet communication tunneling possibilities that can be used in automation systems. Purpose of tunneling is to provide real-time communication over network layer, which is a common problem in automation systems. There are protocols that already offer this to some extent, but their success rate varies [2]. Pure Ethernet communication can provide real-time latencies, but it can be only used in LANs. Tunneling is a method that can be used to solve this problem and allow communication over higher networks. Layer 2 tunneling can be implemented for example in energy distribution networks, smart grids or in any other automation system that has utilizes layer 2 communication. Tunneling provides a way to transport lower level protocols on higher level networks or to transport communication over a non-supported network. A tunnel is a direct connection between communicating devices making the routing of messages simpler and faster. In case of substation and Intelligent electronic devices (IED) communication, the devices can belong to separate local area networks but using a tunnel the LANs can be connected via a virtual private network and the devices can communicate as being in the same LAN. The devices can communicate with layer 2 protocols while the tunneling protocol handles routing over network layer. The benefit in this is that the messages don't require a separate mapping into IP packets and destination address check-up after each hop like in traditional IP routing, and thus it is possible to provide faster communication over network layer using tunneling protocols. [3]

The main focus of this study is in suitable tunneling protocols and communication protocols, but also security and resiliency solutions for layer 2 tunneling are studied. The challenge is to find a suitable solution that meets the requirements from all these areas. To narrow down the vast selection of possibilities, the focus is only in in Ethernet communication and protocols that support it. Also, the studied solutions are limited to open source technologies that can be used without licenses or equipment's from specific manufacturers. This restriction is set so that the results of this thesis can be used by anyone. The future automation systems and electricity distribution networks should be interoperable with each other which makes connecting new customers to the network easier and enables collaboration between energy distributors.

This thesis is composed of information gathered from published studies, researches, articles and books of the subjects mentioned above. Using the gathered information, layer 2 tunneling solution are studied using two use cases. The first use case concentrates on voltage control communication in electricity distribution networks. The second use case concentrates on automated fault isolation and recovery in industrial automation systems. This thesis doesn't contain concrete tests of the found solutions because of the limited time and the amount of work and equipment's needed for setting up an adequate test system with required components and software. A future work would be to build and test the solutions found in this thesis.

This thesis is made for Tampere University of Technology department of Automation Science and Engineering. More precisely the topic of this thesis is related to a FLEXe program, organized by CLIC Innovation, in which the department is taking part in. The purpose of the program is to study flexible energy systems to create novel technological and business concepts enhancing the radical transformation from the current energy systems towards sustainable systems [4]. This thesis is an additional study in respect of the main topic that the Automation Science and Engineering department of TUT is studying.

1.3 Structure

The thesis consists of seven chapters. This Chapter 1 is the introduction to the thesis, explaining the goal and motivation of the work. In Chapter 2, the main parts of layer 2 tunneling are explained. The parts include: Network communication layers, Ethernet protocol, layer 2 and use of tunneling in automation systems. After the second chapter, the reader should have a clear understanding of the topics that the thesis handles.

Chapter 3 starts the examination of suitable protocols for the tunneling solutions. It presents the selected communication protocols that filled the set requirements. Chapter 4 introduces the tunneling protocols that can be used in the final solutions. The protocols were selected by their ability to tunnel Ethernet communication and transports them over network layer. Chapter 5 continues the introduction of suitable protocols by presenting resilience methods and security protocols.

In Chapter 6, the introduced protocols and methods interoperability is considered and suitable layer 2 tunneling solutions are examined. The solutions are studied using two use cases which are coordinated voltage control and automated fault isolation and recovery. Chapter 7 concludes the thesis with the results, overall thoughts about the thesis and what future work could be done based on the results.

2. LAYER 2 TUNNELING

In this chapter, the main parts of the thesis are introduced and their theoretical background explained. At first, network communication layers are explained using a standard model. It should provide an understanding what different functions network communication has and how they work. After that a cursory overview of Ethernet protocol is presented. Lastly, layer 2 and tunneling in general are explained and their role in automation systems is described. There are multiple possibilities how tunneling can be utilized and providing real-time communication is the most important one for this study. The other examples here are meant to give an idea of what kind of other setups are also possible. After this chapter, reader should have an understanding of the different areas that are addressed in this thesis.

2.1 OSI model

Standard method for describing network communication and technologies is to use the Open Systems Interconnection (OSI) model. It is an international standard developed by International Organization for Standardization (ISO) and it divides the telecommunication into 7 distinct layers. The layers can be split into lower layers, which includes layers 1-4, and upper layers, which includes layers 5-7. The lower levels handle the actual transferring of messages and the higher layers consist of application implementation and how the data is presented to the user. The concept of OSI model can be seen in Figure 1.

Layer 1, the physical layer, describes the actual transmission media for transferring communication. It handles the physical connection and the sending of signals. Layer 2 is called data link layer and its purpose is to transmit messages, called frames, over the physical layer. It is also the connection between two directly connected network nodes. In a single node, data link layer is the connection between the transmission medium and the software. Layer 3 is the network layer. It describes routing of network message, called packet, and creating of logical paths between nodes. Layer 4, the transport layer, defines how the data is transmitted or received. For example, layer 4 decides if the data needs to be divided into smaller pieces before sending. Additionally, layer 4 handles the combining of received data pieces and checks the order and integrity of each packet. [5]

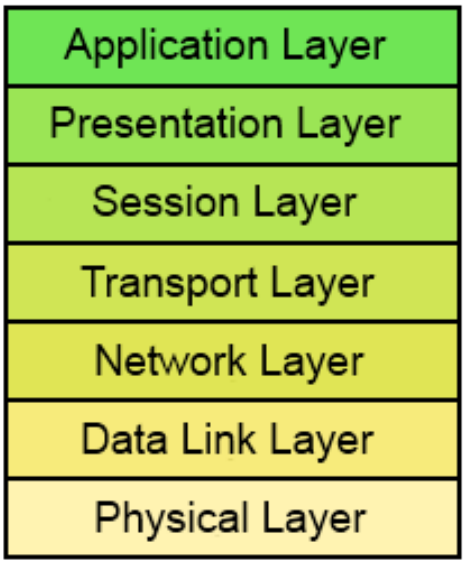


Figure 1 OSI model

Layer 5 in the OSI models is called session layer. It handles the connection between the connected nodes applications. Layer 5 also responsible that the data is sent correctly and that there is no data loss. Layer 6, presentation layer, describes the data representation from application layer format to network format, and vice versa. Layer 6 also handles encryption of the data. Layer 7 is the highest layer in OSI model and it is called application layer. The application layer describes the connection between the user application and the OSI model and offers the services the application needs. [5]

2.2 Ethernet protocol

When looking at the OSI model it is clear that layer 2, being closest to the physical media, offers the fastest communication. But without the additional addressing offered by layer 3, the communication can be only used in local networks. The messages transferred in layer 2 are called frames and their addressing is done using communicating devices unique hardware addresses, also known as Media Access Control (MAC) addresses. Most common layer 2 network standards are the Institute of Electrical and Electronics Engineers (IEEE) 802 standards for LAN and metropolitan-area networks (MAN). The IEEE 802 divides the layer 2 into two sublayers: Logical link control (LLC) sublayer and MAC sublayer. The placement of the sublayers is shown in Figure 2. The LLC is responsible of managing communication protocols and their encapsulation and also handling frame traffic. MAC sublayer governs how devices in a network have access the physical network medium and also packet switching. [6]

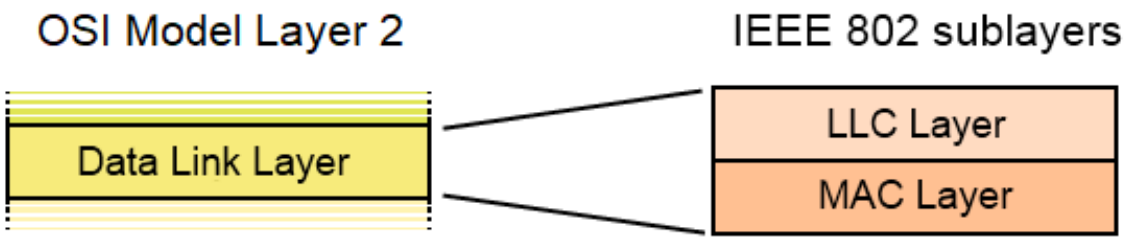


Figure 2 IEEE 802 layer 2 sublayers in OSI model

Ethernet, also known as the IEEE 802.3 standard, is becoming more and more dominant technology when it comes to broadband services for transferring data, voice and video. Already it can be said to be most popular technology in wired LANs [7]. Ethernet itself is a simple protocol, but due to vast hardware support and multiple interoperable security and redundancy protocols, it has been accepted to also safety-critical industrial systems and substation networks [7]. Ethernet is a packet based technology where the devices can send data at any given time. The packets are directed to their destinations with switches that also prevent packet collisions. Addressing is done using MAC addresses. Ethernet has been improved steadily and the data transfer rate has grown greatly. Addition to wired transfer, Ethernet frames can also be transferred using a Wi-Fi/wireless LAN (WLAN), also known as IEEE 802.11 standard. A wireless access point/router/switch/network bridge is needed to transfer Ethernet frames into 802.11 frame form and then sent to the receiving device where they are transferred back to Ethernet frames. This can be problematic due to different frame lengths of the two frames. Wireless network brings own security issues to the system due to the fact that anyone in range of the network can send messages to the access points.

Figure 3 shows the structure of an Ethernet frame. The first 7 octets form the preamble which is used for synchronizing the data transmission. The one octet Start Frame Delimiter field marks the start of a new package. Ethernet frames header constructs of two 6-octet MAC address fields, the destination and source, and a 2-octet length count. The length count bytes can alternatively be used as an Ethertype field. Ethertype is used when Ethernet frames are encapsulated with another communication protocol and it indicates what is the used protocols type. This makes it easy to identify the overlay protocol. Next field is designated to the message data which size can be from minimum 46 octets up to maximum 1500 octets. The last field is the 4-octet cyclic redundancy check (CRC), which is used to check the validity of the package. It protects the package receiver from data corruption or alteration. The Ethernet frame doesn't have a separate end field and the ending is usually marked with the loss of the carrier signal. There are several different types of Ethernet frames from which the Ethernet II is the often used. The difference between the frame types are slight length variation and different start bytes of the data field, but they all can coexist in the same network. If larger data amounts in a single frame is needed there is possibility to use jumbo frames. In jumbo frames the data field size can hold up to 9000 bytes. [9]

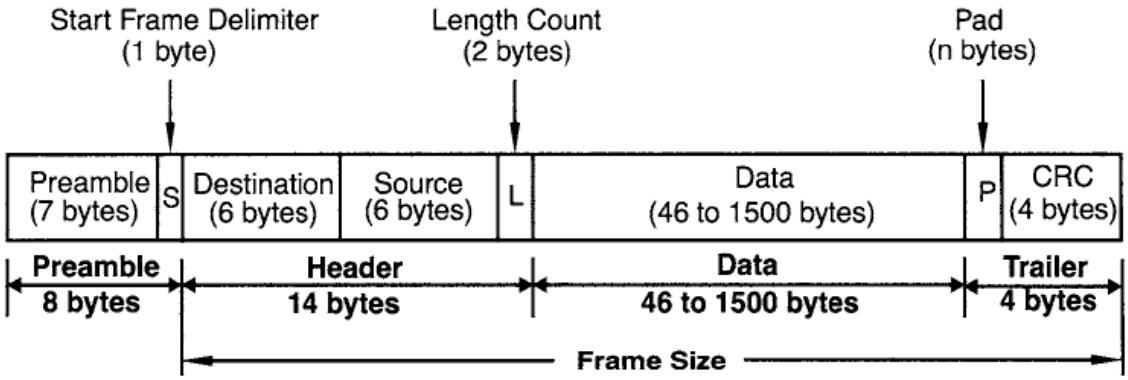


Figure 3 Structure of an IEEE 802.3 frame [10]

There are multiple communication protocols that utilize Ethernet. These protocols can be divided into two groups: those that use purely Ethernet and those that also utilize layer 3 protocols. The former ones use only Ethernet stack and the latter ones can use both layer 3 protocol stack and Ethernet stack. When only Ethernet stack is used the communication latencies are small due to the simple packaging, transmitting and addressing. Due to the small latency Ethernet is the best choice for real-time communication systems. Figure 4 shows the difference in communication paths if only Ethernet protocol is used and if also a layer 3 protocol is used. With pure Ethernet, the communication is directed from the application straight to the Ethernet, skipping the additional layer 3 packaging. The obvious negative point is that pure Ethernet may only be used in when communication in a single LAN is needed. Ethernet is a non-routable protocol and therefore alone it is not suitable for wide area communication. This is where use of tunneling protocols can be used so solve and make real-time communication in WAN possible. It should be noted that there are multiple Ethernet protocols that also utilize layer 3, thus allowing communication over WAN, and some of them can also manage real-time communication [2][6]. These protocols may have limitations and requirements, which may make their usage difficult. Tunneling protocols main difference from those protocols is that they offer a general solution that can be used with multiple communication protocols. Another downside with Ethernet frames is that they are transferred via switches or bridges which direct the package towards their destination. Bridges keep a table of MAC addresses of the network which they update with the messages passed through them. But if a destination address is unknown, they send the package to everywhere in hope that it finds the destination. In case of multiple packages sent everywhere, the network might get flooded and cause delay to time-critical messages. There are solutions that can minimize or even prevent these issues, and some of them are studied later in this thesis. [3]

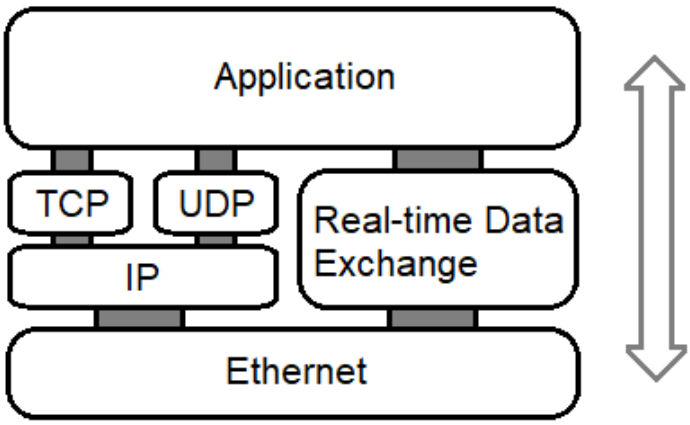


Figure 4 Example of layer 3 and layer 2 protocols stacks

2.3 Layer 2 and tunneling overview

Layer 2 is the second layer in the seven-layer OSI model. Layer 2 is called data link layer and its purpose is to provide a connection between nodes in the same LAN or between two directly connected network nodes in a wide area network (WAN). In a single node, data link layer is the connection between the transmission medium and the software. The functionalities designated to layer 2 are: handling links between network entities, data framing (encapsulate network layer messages into frames that can then be sent across a physical network layer), maintaining flow control and error detection and handling. Layer 2 networks are mostly used in a limited area where devices are located in close proximity. Using a gateway device layer 2 network can be connected to a layer 3 network.

There are several different physical media layer 2 networks can utilize. The most commonly used is copper wire, which is cheap, but needs a proper shielding to prevent electromagnetic interferences. Copper wires are being replaced with optical fiber for its high data bandwidth, minuscule signal reduction over long distances and immunity to electromagnetic interference. Optical fiber is expensive, so it is mainly used in cities and communities where the network users live in close proximity. Third wired transfer option for layer 2 communication is power line communication (PLC). PLC can be a valid option in rural areas, but in urban areas it is not seen as an alternative anymore due to other more capable options. Layer 2 communication can also be transferred via wireless technologies and even radio network utilization is possible. [11]

Tunneling is a method of transferring communication packets between two points. The idea behind tunnels it to provide a service that can transfer a communication protocol over a network which does not normally support it. In other words, it provides access to a non-supported network service. The basic concept of tunneling protocols is to create a direct connection between 2 or more communicating devices across wide area network. In these direct connections tunneling protocols use pre-configured routes to the destina-

tion device. When a lower layer frame reaches the gateway device, also called ingress device, of the tunnel, the tunneling protocol encapsulates the frame with a specific tunneling header and sends it through the tunnel. With the tunneling protocol information added with the header, each router forming the tunnel knows exactly where the packet is going. This makes the routing faster because each device doesn't need to read the address and search for the next hop. The tunnels end device, also called egress device, removes the added encapsulation and the original frame leaves the tunnel. In this thesis's perspective, tunneling protocols are used to send Ethernet frames, or protocol data units (PDU), over network layer without needing to transform them into network layer packets first. Layer 2 tunneling protocols can be used when devices in separate LANs need to communicate with each other. With use of a tunneling protocol the LANs can be connected via a virtual private network (VPN) and the devices are able to communicate as if they would exist in the same LAN. [12]

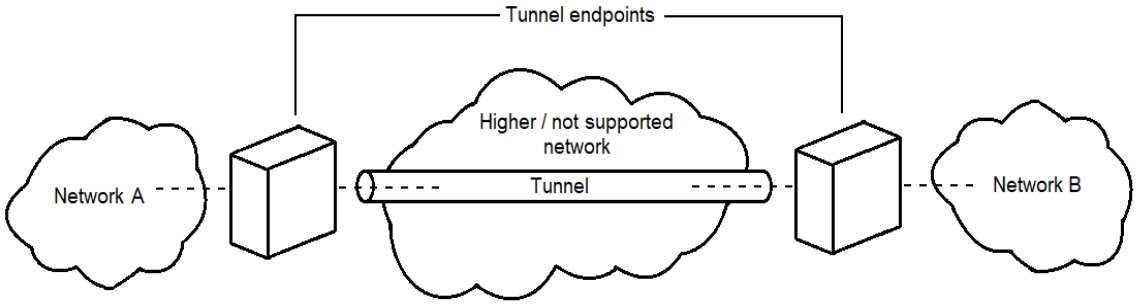


Figure 5 General architecture of a tunnel

A general architecture of a tunnel can be seen in Figure 5. Depending on the tunneling protocol, the tunnel can be constructed between customer edges (CE) or provider edges (PE). In layer 3 tunneling protocols, the tunnel starts at CE routers and they handle the encapsulation and de-capsulation of packets. In layer 2 tunneling protocols, the tunnel starts at PE routers and they handle the encapsulation and de-capsulation of the transmitted packets. The encapsulation makes it possible to transfer layer 2 frames over layer 3 network. The encapsulation varies depending on the used tunneling protocol and what is the layer 3 networks type. When the encapsulated frame reaches its destination PE router, the tunneled packet is de-encapsulated and the original message is forwarded to the connected CE and from there to the destination device in the new LAN. Benefit of using a tunneling protocol is that the original message stays unchanged. When a tunnel is set up, a pre-configured route between the end points is created, making the routing of messages simpler and faster than for example with traditional IP routing, where the destination address is checked after each hop. If a failure occurs in the tunnel route, a new route can be calculated. [12]

Layer 2 tunneling can be utilized in any automation system that deals with data link layer communication. One such system is an electric power distribution network, more precisely the LV area where secondary substations (SS), IEDs and distributed genera-

tors are located. A tunnel can be set up to provide a direct between these devices. The SS is the connection point between a LV and a medium voltage (MV) area. The existing devices (IED, smart meters, DG equipment, houses, etc.) in LV area form a LANs in which they communicate with each other. Depending on the area, a whole LV grid can be just one LAN or it have multiple LANs. One LAN can consist of, for example, a group of houses or buildings in a certain street, or it can be an area of just energy consumers or have also DG equipment. These LAN's or LAN are connected to a SS. SS controls both the data and electricity flow to the LV area from MV area and from a primary substation. An example of a LV distribution network can be seen in Figure 6. [13]

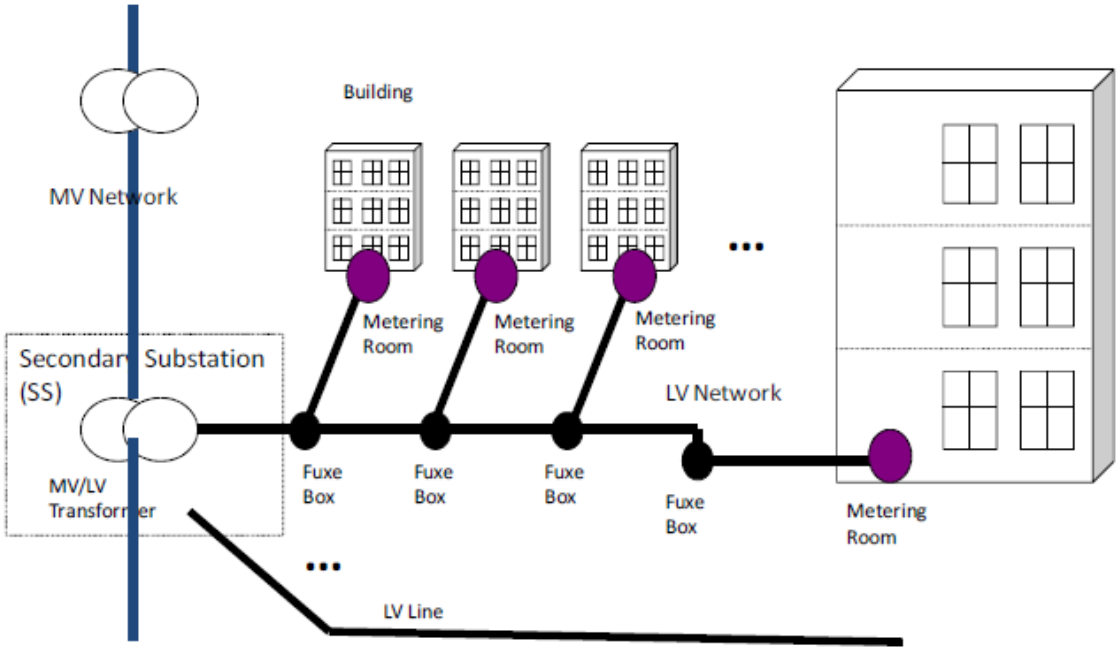


Figure 6 Typical LV distribution system. [15]

In industrial automation systems or distributed networks, tunneling can become beneficial when real-time communication is needed. As mentioned before, Ethernet communication can pass the requirements of time critical communication. But problems arise when real-time communication between separate LAN's is needed. Protocols that try to provide this has been developed, but their implementation requirements and system compatibility varies greatly and they might not be suitable for all systems. They also have the same downside: mapping frames into network layer packets and routing them individually. With use of tunneling, separate LANs can be connected together in a VPN and can the devices can communicate using layer 2 protocols, without knowing that they are don't physically exist in the same LAN. Routing is done by the preconfigured route set up by the tunneling protocol.

One of the crucial part of the layer 2 tunneling system design are the routers and gateways. Good routers and gateways can provide security and resiliency to the whole network. Routers and gateways role is to direct messages from a LAN to outside and also

receive messages from outside. according to their intended address. The addresses are received from the messages and compares them to the routers own constructed list of addresses. Routers handle traffic between similar networks and gateways handle traffic between dissimilar networks. Inside a LAN, switches are used to direct messages and prevent broadcast and multicast messages from leaving the LAN. Most routers and gateways have built in security features like a firewall, security protocols (like Wi-Fi Protected Access (WPA) and WPA2 authentication protocols for Wi-Fi), etc. Also, other devices that provide access to Internet, WAN or Metropolitan Area Network (MAN). Routers, routing switches, integrated Access Devices, multiplexers, and various MAN/WAN devices. [1]

An example case when tunneling communication between LANs can be beneficial, is when a connection from one LAN to a secondary substation is disconnected and there is no way of informing about the problem. In this case, a horizontal connection to an adjacent LAN can be created, or used if a connection already exists. This connection can be constructed using a tunneling protocol allowing the LANs to form a VLAN. The messages can then get routed to the SS through the adjacent LAN. In a larger scale, this same scenario can be applied to a situation when communication between different electricity distributers (ED) is needed. If one EDs power line in a LV area is cut off, the area can get isolated and the customers are left without a connection. In this case a connection can be created to a neighboring ED and requesting a connection to their electricity network [13]. This scenario would reduce the costs and down time of customers tremendously, but it requires interoperability between different device vendors and EDs, and also intelligent electricity networks to be built to handle this.

3. COMMUNICATION PROTOCOLS

There are many communication protocols that can be used in automation systems. This thesis concentrates in the ones which utilizes the IEEE 802.3 (Ethernet) standard. The focus is more in real-time protocols that can manage time-critical messages, and therefore it is possible to see if with tunneling real-time communication can be achieved over network layer. The studied layer 2 protocols were chosen by 3 factors. First, the protocols should be widely used and may still be under development. This guarantees that they won't become obsolete soon and can be enhanced still. Second, they are open source and vendor independent. This makes it possible for anyone to use them and improves the interoperability of devices. And the third factor is that they provide decent security and/or additional security protocols and methods can be applied to them.

In this Chapter, communication protocols that are suitable for layer 2 tunneling and that suit the scope of the thesis are introduced. Their communication requirements, limitations and compatibility are in the key role. Protocols presented in subchapters 3.1.1 - 3.1.3 are commonly used in distributed networks. Protocols presented in subchapters 3.1.4 - 3.1.6 are Industrial Ethernet protocols. There are multiple Industrial Ethernet protocols which are all developed to provide real-time communication. The protocols presented in this thesis suit the best if regarding the requirements listed above.

3.1.1 IEC 61850

IEC 61850 protocol is a globally accepted standard which is developed by the IEC Technical Committee 57 (TC 57). It is based on the Utility Communications Architecture and defined to be a uniform and future-proof solution for automation systems using Ethernet-based communication. The information models and information exchange presented in the standard were developed for communication between control centers and communication between control centers and substations. The development of the IEC 61850 standard started already in 1994-95, but the first edition was published not until 2005 [14]. Although, after it was introduced, the standard was noticed to also be useful in application outside substation automation systems. This was the motivation to further develop the standard so that it could be utilized throughout the power distribution system [15]. The development and growing popularity of distributed energy technology has also lead the IEC 61850 to that direction, and new standards define data models specifically for DE technologies. The list of IEC 61850 standard documents can be seen in Figure 7 and the related standards are listen in Appendix A.

The IEC 61850-1 standard defines goals for the IEC 61850 that should be fulfilled. Most important goals regarding this thesis are [16]:

- Communication profiles should base on the IEC/IEEE/ISO/OSI communication standards if possible.
- Used protocols should be open and support the function of devices in their description. Also adding new features should be possible.
- Syntax and semantics of the communication should be based on common data objects that belong to the network.
- Communication standard should be based on the objects that are relevant to the needs of the electric power systems.

Part #	*Title*
1	Introduction and Overview
2	Glossary of terms
3	General Requirements
4	System and Project Management
5	Communication Requirements for Functions and Device Models
6	Configuration Description Language for Communication in Electrical Substations Related to IEDs
7	Basic Communication Structure for Substation and Feeder Equipment
7.1	- Principles and Models
7.2	- Abstract Communication Service Interface (ACSI)
7.3	- Common Data Classes (CDC)
7.4	- Compatible logical node classes and data classes
8	Specific Communication Service Mapping (SCSM)
8.1	- Mappings to MMS(ISO/IEC 9506 – Part 1 and Part 2) and to ISO/IEC 8802-3
9	Specific Communication Service Mapping (SCSM)
9.1	- Sampled Values over Serial Unidirectional Multidrop Point-to-Point Link
9.2	- Sampled Values over ISO/IEC 8802-3
10	Conformance Testing

Figure 7 Structure of IEC 61850 standard [16]

For client-server communication the IEC-61850 uses Manufacturing Message Specification (MMS). The abstract services are mapped into MMS protocol. MMS was originally designed for manufacturing systems, as the name suggests, but because it supports the IEC 61850's complex naming and service models it was chosen to be used. Other reason was that it is an ISO standard protocol and designed as vendor-neutral. For hori-

zontal communication, the IEC 61850-8-1 standard is the most meaningful. It defines Generic Object Oriented Substation Event (GOOSE) messages that enables Ethernet based messages across a LAN. The GOOSE messages are associated with a peer-to-peer model for Generic Substation Event (GSE) services that are related to time-critical and reliable communication between protection IEDs. Other GSE type message type is Generic Substation State Event (GSSE). It is a binary-only message type, but older and slowly being diminished by the popularity of the more flexible [17]. The IEC 61850 also includes another real-time, Ethernet based, peer-to-peer communication method in addition to GSE called Sampled Values (SV). SV peer-to-peer messaging is used in the process level for communication between IEDs inside substations or switching stations and the relay in the control building. The messages are digitized instantaneous values. SV is a non-routable protocol so it is only designed to be used inside a LAN. Of course, with tunneling the SV messages can be sent over the network layer.[18][19]

The three peer-to-peer communications mechanisms (GOOSE, GSSE and SV) are all multicast message services and use an unconfirmed publisher-subscriber service model. The multicast model is connectionless so to speak, which means that the sender sends frames to a multicast address but doesn't know who receives the messages. It also means that any device can be a subscriber to any known multicast address. GOOSE and SV communication mechanisms are time-critical protocols and by directly mapping to the Ethernet frames, the latency has been managed to keep small enough to meet the requirements for protection automation. The different communication mapping methods are shown in Figure 8. Additionally, the IEC 61850 communication services change the traditional protection schemes. They reduce cost of systems design, installation, deployment and maintenance. Also ease of operation and the reliability of the system can be increased. [17].

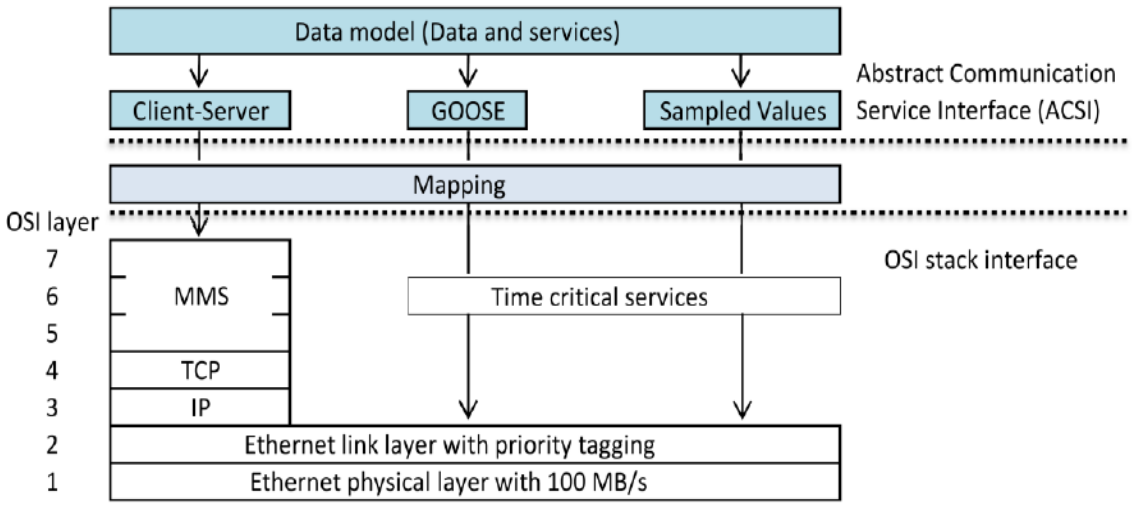


Figure 8 IEC 61850 data model and service mappings [9]

IEC 61850 GOOSE

The GOOSE communication runs directly on top of Ethernet. It has its own Ethertype value which can be used to identify GOOSE messages. As a non-routable protocol, the GOOSE communication can only be used inside a LAN or other type of layer 2 network. A separate mapping or encapsulation, which tunneling protocols provide, is required for GOOSE messages to access network layer and reach other LANs. The messages are sent in multicast form and they can transport both analog and digital values.

Benefits of GOOSE protocol [20]:

- Directly mapped on to the Ethernet layer which makes it suitable for time-critical messages regarding the message processing time.
- Because GOOSE uses standard Ethernet, it gets improved as Ethernet is further developed.
- Uses multicast messaging mode and therefore reduces the data traffic and load in IEDs because only subscribers will open the message.
- Doesn't have a built-in handshake mechanism which improves the speed of the data exchange
- Has a built-in 'time allowed to live' parameter which is used to set each packets longevity in the network.
- To guarantee high reliability, messages are repeated as long as a state persists. The time between messages is set with a MaxTime parameter.
- One message from an IED can contain all the required data related to the protection scheme. This reduces the amount of traffic.
- For dependability and security, each message has a 'hold' parameter which determines the time a message will live and later will expire if the next message with the same status is received or a new message is received before the hold time ends.
- Can utilize the advanced configurations of Ethernet frames, for example priority tagging and VLAN.

Sampled Value

The SV protocol is defined in IEC 61850-9-2 standard which defines the provided services and needed requirements, which are very tight due to SV being a time-critical protocol that needs solid reliability. The measurement values must be in chronological order so none of them is allowed to disappear or be delayed compared to other measurements. The purpose of SV service is to transmit analog values, or samples, from measurement devices in digitalized IEEE 8802-3 standard form. Most commonly it is used to send current and voltage values. SV protocol has its own Ethertype value to identify it from other Ethernet frames same way as GOOSE. Also, addition to sending multicast messages, SV messages can be sent in unicast form, which is meant to be received by only one particular device. Similar to GOOSE, SV is a non-routable protocol and can only be used inside a LAN or other type of layer 2 network. [21]

3.1.2 IEC 60870-5-104

IEC 60870-5 standard is developed by the IEC TC57. It is a communication profile designed to be used in Supervisory Control and Data Acquisition (SCADA) automation systems for wide variety of control and monitoring communication. IEC 60870-5 is one part of the 60870 standards and it was first published in 1990. The part 5 includes seven base definition documents and four companion standards: [22]

- IEC 60870-5-101
- IEC 60870-5-102
- IEC 60870-5-103
- IEC 60870-5-104

The IEC 60870-5-101 and IEC 60870-5-103 standards are dated but still used. The IEC 60870-5-101 defines monitoring and controlling transmission for control systems and equipment. The IEC 60870-5-103 defines information exchange between protection equipment and control system. Both the IEC 60870-5-101 and IEC 60870-5-103 use serial line communication and are therefore not studied in this thesis any further.

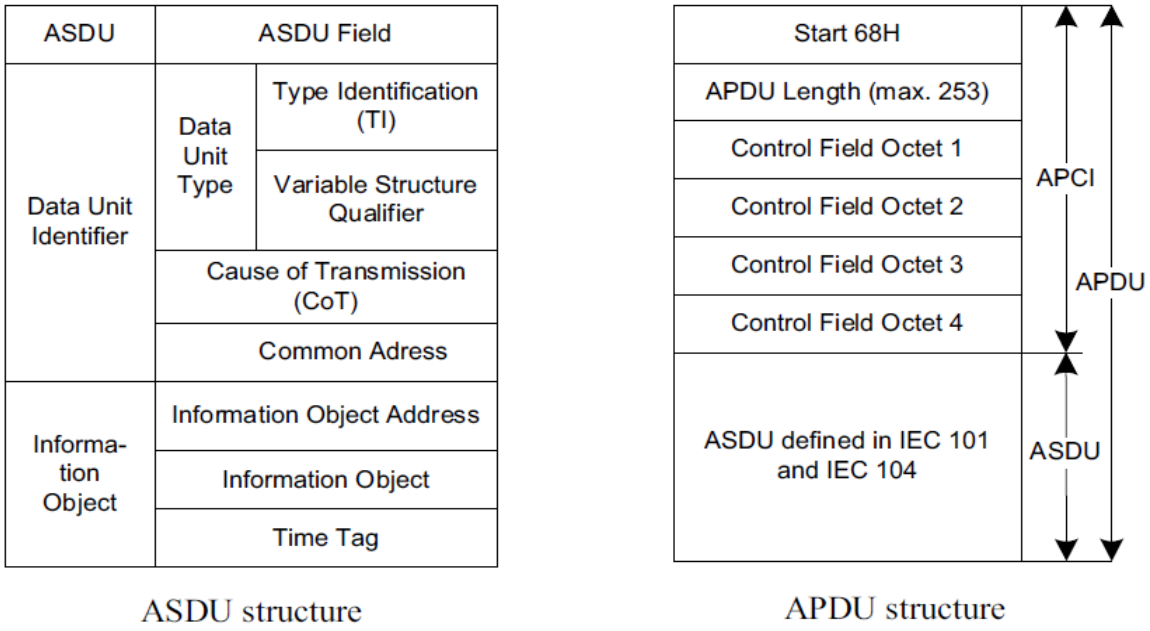


Figure 9 IEC 60870-5-104 ASDU and APDU structures [23]

The IEC 60870-5-104 is basically the same as the IEC 60870-5-101 protocol but with added Transport Control Protocol (TCP)/IP protocol transport function. This makes the 60870-5-104 protocols utilize the layer 3 (network layer) in the OSI-model. There are also some information types and configuration parameters that exist in IEC 60870-5-101 but not in IEC 60870-5-104, for example short time stamps in messages. The IEC

60870-5-104 defines monitoring and controlling transmission for control systems and equipment. The main advantage over the IEC 60870-5-101 is that in IEC 60870-5-104 the communication is much faster due to the simultaneous transmission of the standard network. The protocol defines usage of all OSI model protocol layers, except layers 5 (session) and 6 (presentation). In OSI model layers 2 (data link) and 1 (physical) IEC 60870-5-104 can utilize Ethernet or direct connect with Point-to-Point protocol, which won't be discussed in this thesis. The protocol was first published in 2000 and it is still widely used in SCADA systems. Interoperability of different vendors using IEC 60870-5-104 is ensured with an interoperability list defined by the standard [22] [23].

IEC 60870-5-104 in electricity networks is usually used to transfer data from substations to the operator systems. It can also be utilized in communication between a substation and an IED, a remote terminal unit (RTU), a programmable control unit (PLC) or a meter. Communication is based on sending Application Service Data Units (ASDU) constructed in the application layer. After ASDU is constructed, an Application Protocol Control Information structure is attached to the ASDU. Together they form the basic IEC 60870-5-104 message format called APDU. The structure of each unit can be seen in Figure 9. [23]

3.1.3 Distributed Network Protocol

Distributed Network Protocol (DNP3) is an open communication protocol based on early work of the 60870-5 standard developed by the IEC TC57. It is specified as a layer 2 protocol and mainly used in communication between substations, IEDs, RTUs and control stations in automation systems. Originally developed by Harris, Distributed Automation Products, DNP3 has been developed by the DNP3 Users Group since 1993. The transmission method can be serial line, mainly used for communication inside substation, or Ethernet and additionally TCP/IP, for communication outside substations. Same way as IEC 60870-5-104 the DNP3 is considered as a SCADA protocol. [24][25]

The DNP3 protocol standard defines usage of OSI model layers 1 (physical), 2 (link) and 6 (application). It also provides its own transport layer functions similar to the OSI model layer 4. The transport layers main purpose is to break the message fragments from application layer to sizes that can be transmitted by the link layer, which is 250 data bytes. The application layer breaks messages into fragments which are usually from 2048 to 4096 bytes [25]. This can be a problem to the communication because every fragment of 2048 bytes have to be divided into 9 frames by the transport layer. If one frame is lost or delayed the original message can't be reconstructed. Especially in systems with high availability this must be taken into account. Solution for this could be sending smaller messages.

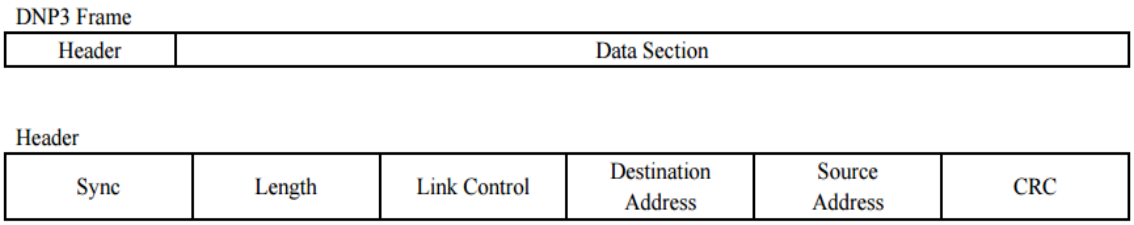


Figure 10 DNP3 frame structure [25]

DNP3 protocol has two different methods regarding data transfer from slave to master. First method is by polling, in which the master sends request for each value it wants to read. Second method is to send unsolicited messages from slave to master. The slave sets events for data objects which sends its data value to the master when defined change happens, for example a change in state. To set a message priority the DNP3 defines 3 classes. Class 1 messages have the highest priority and class 3 the lowest. In DNP3 it is also possible utilize the class value in polling request data from each data point with a certain class value.

As default functionality, DNP3 protocol is defined to provide data fragmentation, error checking, message prioritization and link control for data transmission. As a security measure, DNP3 uses CRC checks. In most protocols one set CRC bytes are added to the end of the frame, but in DNP3 frame a CRC check is added into the data field after every 16 data bytes. This gives high security to the data reliability for each frame and the number of data bytes can still be the maximum 250 bytes. To enhance security of DNP3, in 2010 the standard defined use of Secure Authentication (SA) version 2 similar to the IEC 62351-5 standard. The latest DNP3 standard IEEE 1815-2012 upgraded the security more by defining usage of SA version 5. [26]

3.1.4 Modbus TCP

Modbus is a transmission protocol developed by Modicon, now known as Scheider Electric. It was first published in 1979 and it is an open protocol for process control systems. It is now managed by the Modbus Organization. Modbus is an application layer (OSI model layer 5) protocol meaning that the PDU's information are handled by the application software. It also means that it is independent of the underlying physical layer and therefore open for different solutions. Modbus is usually used to handle PLC device communication but for its flexibility utilization possibilities are vast. Modbus is considered as very easy to implement, efficient and flexible protocol for multi-vendor systems. Although being such an old protocol, it is still widely used around the world and it seem to find its way even to modern systems, like Internet of Things applications. [27]

There are two different data transfer version Modbus protocol, serial port and TCP/IP communication. Messages can be mapped between the two modes because the protocol defines a PDU that both modes use. Although an interconnection device must be used when connecting TCP network and serial line. In this thesis, only Modbus TCP is studied. Original Modbus frame has an address and error check fields added to create a full message, also called an application data unit (ADU). In Modbus TCP, these additional fields are not used but a 7 bytes long Modbus application protocol header field is added in front of the PDU instead to construct a Modbus TCP ADU. Figure 11 shows the structure of the ADU. The Modbus TCP ADU is then embedded into the standard TCP frames data field. Modbus TCP supports the basic IEEE 802.3 Ethernet in layers 2 and 1 and therefore doesn't need any special devices or equipment when transferring frames through Ethernet. [28][29]

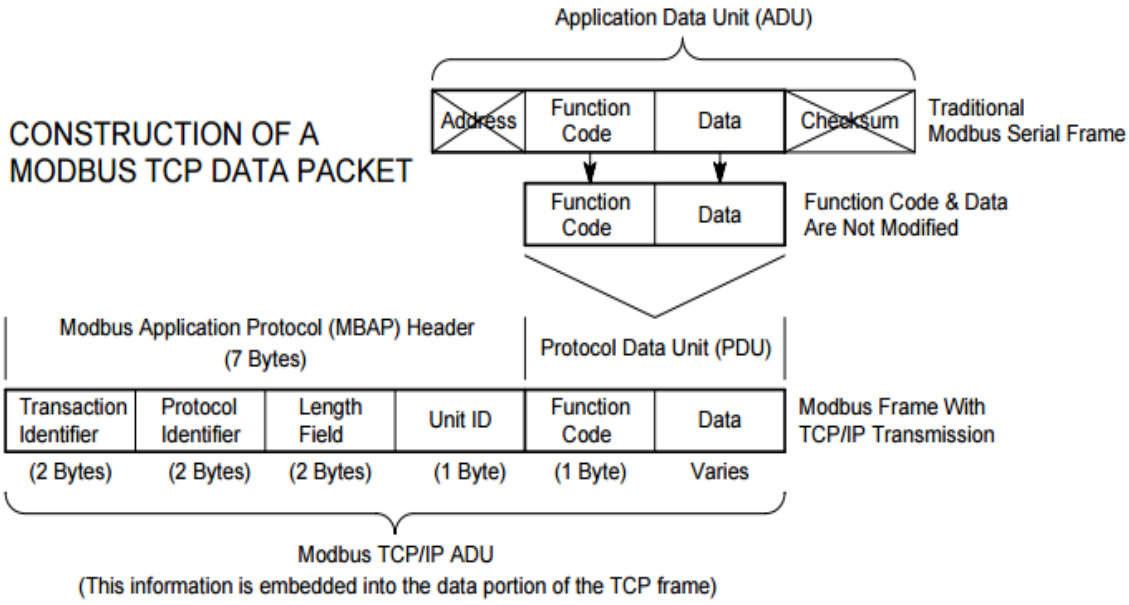


Figure 11 Structure of Modbus TCP ADU [28]

Modbus TCP offers a basic master slave communication between 2 or multiple devices. Because of its popularity and vender independency there are countless of applications and devices supporting it. The master-slave communication is based on predefined function codes which are defined in the Modbus protocol standard [29]. One limitation of Modbus is that the master must send a request/poll to initiate response from a slave, so Modbus doesn't support unsolicited data traffic. Also, the certainty that the messages reach each end is solely the master's responsibility, meaning that a Modbus slave device doesn't have any data acknowledgment functionality. [27]

3.1.5 Ethernet/IP

Ethernet/IP is an open industrial networking standard. It is an application layer protocol developed to bring a flexible Ethernet solution to Industrial Automation [30]. It was

first developed by Rockwell Automation but is now managed by Open DeviceNet Vendors Association (ODVA). Ethernet/IP supports practically all the transport and control protocols used in the traditional Ethernet. This makes it usable with most of the available Ethernet devices in the market and thus has a huge advance over more restricted protocols. Ethernet/IP also defines usage of TCP/IP suite. In upper layers (OSI model layers 5, 6 and 7) Ethernet/IP uses Common Industrial Protocol (CIP), which is a communications suite for transferring data in industrial automation systems. In layers 3 and 4 use of standard TCP/IP and User Datagram Protocol (UDP)/IP stacks is defined. In Physical and Data Link Layers Ethernet/IP uses Ethernet (IEEE 802.3) standard. [30]

In Data Link Layer Ethernet/IP follows the IEEE 802.3 standard and therefore it supports most of Ethernet hardware. It uses the traditional Carrier Sense Multiple Access With Collision Detection (CSMA/CD) media access mechanism for collision detection and handling. The Ethernet/IP frame structure is almost identical to the standard Ethernet frame (Figure 3), the only difference being that the 2 length bytes are used to present the Ethertype of the frame. The payload field can hold data from 46 bytes up to 1500 bytes, which is the same amount as the regular Ethernet frame. [31]

Ethernet/IP can be used in time-critical systems when implemented correctly. This requires use of CIP and its extensions, mainly CIP Motion, CIP Sync and CIP Safety. The CIP is an object-oriented protocol in which all device in the network are defined as group of objects. It provides the connection between devices across multiple networks. The devices in the network are described by structure, functionality and operations. Three mandatory objects that must exist in a network are Identity, Message Router and network specific objects. Additional objects are Application objects and Vendor-specific objects. The CIP Motion technology provides a real-time, closed loop distributed motion control solution. The CIP Motion extension uses application profiles that are used to define the technology [32]. The CIP Sync extension provides a time synchronization technology for the Ethernet/IP. With it, it is possible to achieve real-time synchronization between distributed devices [32]. CIP Safety technology can provide a fail-safe communication between the network nodes. It can also enhance the implementation of safety devices into the network. The CIP extensions can also be used together providing the wanted features for each system. [30]

3.1.6 PROFINET

PROFINET is an open communication standard for industrial Ethernet and its designed mainly for data collecting and device control in automation systems. PROFINET is standardized in Fieldbus standards IEC 61158 and IEC 61784. It is currently being maintained by the PROFIBUS & PROFINET International community. Benefits of using PROFINET are the low installation, engineering and maintenance costs and high system availability. [34]. Also, its modular function building makes it suitable for multiple devices and systems. In PROFINET all communication is transferred through the

same cable. Copper and fiber-optic cables are supported. PROFINET has two modes with different focuses: PROFINET IO (Input/Output) and PROFINET CBA (Component Based Automation), which can be used separately or together.

PROFINET IO focuses on programmable controller data exchange with cyclic data transfer over Ethernet. It uses a provider/consumer model and requires pre-configured data structures and meanings on both the controller and the controlled device. PROFINET IO defines three device classes for communication exchange: IO-Controller (typically a PLC device), IO-Device and IO-Supervisor (can be a monitoring computer, HMI device or programming device). For the communication over Ethernet it has two channels: Real Time channel and Isochronous Real Time channel. The Real Time channel is used in standard cyclic data transfer and alarms. The Isochronous Real Time is a high-speed channel meant for cyclic data transfer for critical operations, like Motion Control applications. In PROFINET IO time critical systems communication can be improved by using Dynamic Frame Packing. The system configuration is done by using a configuration tool, which is defined as a IO-Supervisor class, and XML (Extensible Markup Language) based Generic Station Description files. [35]

PROFINET CBA is, as the name suggests, a component based communication standard for controlling, accessing and configuring devices in modular automation systems. Its main base comes from Distributed Component Object Model (DCOM), which is standard from Microsoft, and Remote Procedural Call technologies. With DCOM the data is encapsulated into objects. For layer 3 communication it uses TCP/IP technology and the regular TCP/IP stack. On Layer 2 the standard Ethernet is used. PROFINET CBA can also handle real-time communication. [35]

4. TUNNELING PROTOCOLS

In this chapter, the tunneling protocols are introduced and their structure explained. The protocols were chosen using several requirements: Tunnel layer 2 communication over layer 3, ability to encapsulate Ethernet frames and their suitability for automation and control system communication. At the end of this chapter, a few tunneling protocols that didn't fill the requirements are shortly introduced.

4.1.1 Layer 2 Tunneling Protocol version 3

The Layer 2 Tunneling Protocol (L2TP) is a VPN solution that offers a mechanism for tunneling OSI model layer 2 frames over an IP network. The Layer 2 Tunneling Protocol version 3 (L2TPv3) is the newest version of the L2TP and it is developed by the Internet Engineering Task Force (IETF) Software group. L2TPv3 uses an encapsulation technique in which the layer 2 frames are encapsulated inside L2TPv3 frames when tunneled. Originally designed to be used with Point-to-Point Protocol, it has been developed to support multiple other layer 2 protocols. The L2TP is a combination of Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding protocol (L2F). New features in the version 3 includes support of Ethernet Virtual Local Area Network (VLAN) and Ethernet Port-to-Port and the ability to transfer Layer 2 frames, including Ethernet, Frame Relay and ATM) directly over IP network. On the downside L2TPv3 only supports point-to-point tunnels and not multipoint tunnels. [36][37]

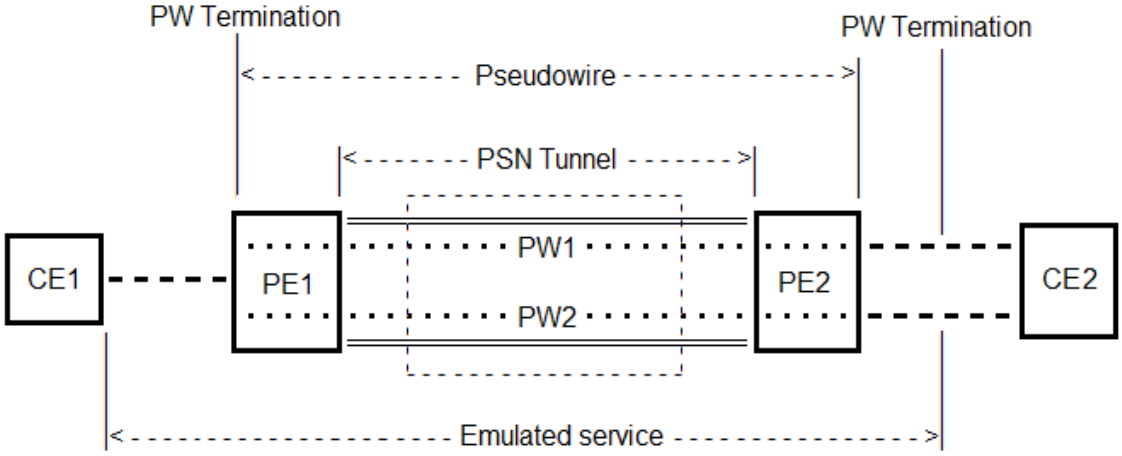


Figure 12 PWE3 pseudowire model [38]

The steps for creating a L2TPv3 tunnel is to establish a Control Connection and establish a Session. The Session includes the tunnels pseudowire, which is an emulated direct

link between two endpoints. For transferring Ethernet frames, the pseudowire follows the Pseudowire Emulation Edge-to-Edge (PWE3) architecture. Figure 12 shows the general model of a PWE3 based pseudowire. In L2TPv3 the two endpoints, or PE are called L2TP Control Connection Endpoints (LCCEs). The structure of the LCCE can be seen in Figure 13. The LCCE has two types: L2TP Access Concentrator (LAC), which is a point that connects L2TP session directly to a layer 2 network entry device, and L2TP Network Server (LNS), which ends the L2TP session but forwards the de-capsulated packets on as network packets. Each LCCE can be a LAC or LNS, or both if they have more than one Session. The L2TPv3 may also have a pre-processing block, Native Service Processing (NSP), which consist of functions like overwriting, stripping and adding VLAN tags. These operations are done to the frames before they are moved to/from the CE. The pre-processing functions depend on what Ethernet technology is being used. After the LCCEs have established a Control Connection they can establish a Session using an Incoming Call three-way handshake. The information needed in the handshake are Pseudowire Type, Pseudowire ID and Circuit Status Attribute Value Pair. When Ethernet frames are tunneled, the Pseudowire Type can be either Ethernet port or Ethernet VLAN. A Control Connection may have multiple Sessions between two LCCEs. If a Session is closed, the linked pseudowire must also be shut down. [36][39]

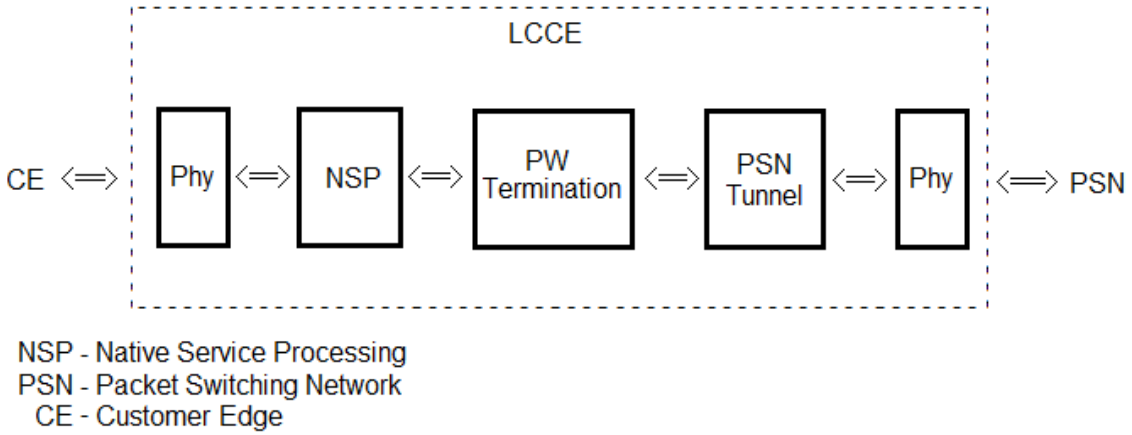


Figure 13 L2TPV3 LCCE structure [39]

The L2TPv3 pseudowire communication has two message types which are control and data messages. The control messages are used for the Control Connection and session handling. The control messages are:

- Call messages for setting up the L2TPv3 Session and the Ethernet pseudowire between the LCCEs.
- Control Connection Keep-alive messages: Used to monitor link statuses.
- Set-Link-Info messages: Used for sending Ethernet link statuses between LCCEs. The Set-Link-Info messages can be sent from either LCCE.

The data messages are used to encapsulate Ethernet traffic into L2TPv3 frames and transfer them over the L2TPv3 session. The encapsulated frames are then sent as single

packages to the remote LCCE, where they are de-capsulated and sent forward as Ethernet frames. The encapsulation is done so that the preamble and CRC fields are removed from Ethernet frames and they are otherwise left unchanged. Then an IP header and additional L2TP session header are added to the frame. The fields in the session header depends if IP or UDP is used as the tunnels backbone. The L2TPv3 encapsulation fields for UDP and IP data messages are shown in Figure 14 and Figure 15 below. The L2-Specific sublayer field consists of control fields for the tunneled frames, such as sequence numbers. Tunneling over UDP is optional for L2TPv3, but tunneling over IP is mandatory. By using UDP it can be easier to pass through firewalls and address translations, but sending packages directly over IP offers higher efficiency and less restrictions. On the other hand, UDP provides a checksum for data integrity check, which the IP lacks. [36][39]

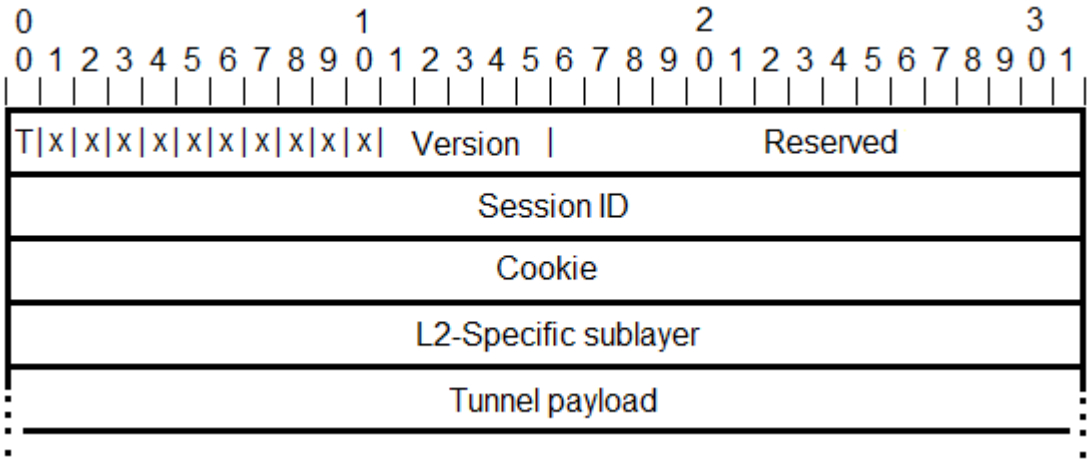


Figure 14 L2TPv3 UDP encapsulation fields. Original image from [39]

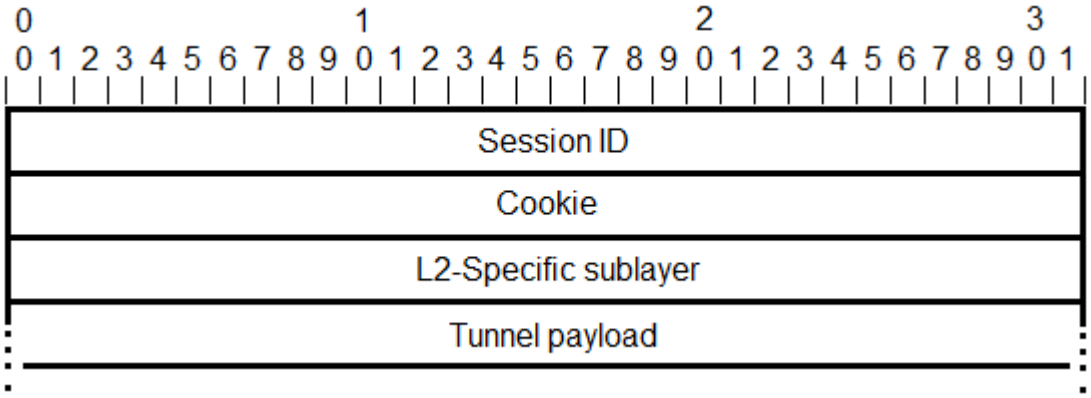


Figure 15 L2TPv3 IP encapsulation fields. Original image from [39]

Regarding the security of L2TPv3, it doesn't have any kind of built-in integrity check for data messages. The PWE3 doesn't provide any kind of integrity or confidentiality services either, so adding separate party security is recommended. Additionally, when the CRC and preamble are removed from the transferred Ethernet frames, it also removes their integrity proof across IP network. Only the Session ID and Cookie fields of

the L2TPv3 header can be used to check if a data message has been damaged or corrupted, but they only check the header. As for control message integrity and message authentication, a password must be shared between the LCCEs. The L2TPv3 standard [36] also states that "The L2TP data channel does not provide cryptographic security of any kind", which means that a third-party security must be used. The standard defines support for IP Security (IPSec) as a mandatory requirement for L2TP systems. The IPSec is further explained if Chapter 5.2.2.

To add resiliency for the L2TPv3, various protocols can be utilized. For example, one option for fault detection and diagnostics mechanisms between the ICCEs is Virtual Circuit Connectivity Verification (VCCV). If VCCV is used the failover must be detected with a separate protocol and one option is to use the Bidirectional Forwarding Detection (BFD) protocol. [40] also describes a 'failover' extension for L2TP. The concept is to create two end points, active and passive, for the L2TPv3 tunnel. When a failure occurs in the other end point, the tunnel is moved to the second end point. The end points can be located in the same physical device, or in different devices. Other suitable resiliency protocols are explained more in chapter 5.1.1. But as a warning, the [38] states that "A number of IETF standards employ relatively weak security mechanisms when communicating nodes are expected to be connected to the same local area network. … The relatively weak security mechanisms represent a greater vulnerability in an emulated Ethernet connected via a PW". [41]

4.1.2 Ethernet over Multiprotocol Label Switching

Multiprotocol Label Switching (MPLS) is a routing protocol that offers fast routing of packets across a network. It is a router-based protocol and it requires compatible routers to work. It is not an IP-based protocol and it uses its own specific MPLS based network and label stack. MPLS is an open standard and it is still developed by the IETF MPLS Working Group. It is based on Toshibas Cell Switch Router idea that was later developed to the multiprotocol label switching concept. In regular IP routing, the packets network address is read after each router hop to determine where it should be forwarded next. In MPLS, labels are added to the transferred packets. The attached labels have the information where the packet is going and the address from the packet itself is not read. For transferring Ethernet frames over network layer MPLS over pseudowire must be used. The method is called Ethernet over MPLS (EoMPLS). [42][38]

The pseudowire service that EoMPLS uses is an emulated Ethernet point-to-point service and it follows the architecture of PWE3. The PWE3 network model builds the emulated service from exactly one customer network edge to another, so that everything in between is inside the emulation. The architecture is the same as with L2TPv3 and the structure of the emulation model seen in Figure 12. The actual pseudowire is constructed around a MPLS tunnel, including the two PE routers. The pseudowire is set up and maintained with the Label Distribution Protocol (LDP), which is a protocol specified to

exchange information between routers in MPLS network. The routers must support MPLS, and these routers are referred as Label Switching Routers (LSR). The structure of PEs in EoMLPS are slightly different than the L2TPv3 LCCEs and their composition can be seen in Figure 16.

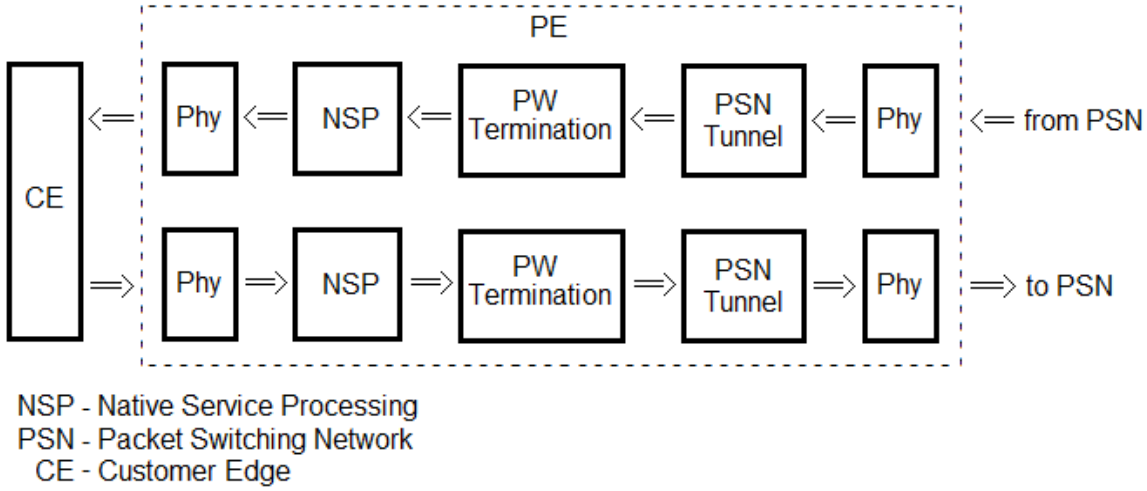


Figure 16 PE structure in MPLS pseudowire. Original image from [43]

The pseudowire is established with a fixed type that cannot be changed afterwards without creating a new session. The MPLS has two Ethernet pseudowire types: Ethernet Tagged Mode, which requires that each Ethernet frame must contain an 802.1Q VLAN tag, and Ethernet Raw Mode, a VLAN tag is not required, but may exist. The handling of the transmitted frames is different depending on which mode is used. If Ethernet Raw Mode is used all received frames are transmitted to the specific PE using a single pseudowire. If some error is noticed in the Ethernet port an error status is sent to the corresponding remote PE. Also, if the frame has an additional VLAN tag (also called a service-delimiter tag) that was attached by some customer service, it is removed before the frame is sent forward. In Tagged Mode if a service-delimiter tag doesn't exist, a PE attaches a temporary self-created tag to the frame. The Ethernet frames encapsulation process in MPLS has the following steps:

- The preamble and CRC are removing the from the frame.
- An optional control word field is added. The control field provides sequencing service to the transmitted frames. It is a service MPLS PSN doesn't have and it prevent the packets from getting disordered during transportation.
- A pseudowire demultiplexer field, also called a pseudowire label, is attached.
- A tunnel encapsulation is added. This depends on how the PSN was set up.

All the attached additional fields are removed by the PE when the packet is received. The CRC is the recreated to the Ethernet frame before it is sent forward to CE. [43][44][42]

For changing information between routers, EoMPLS utilizes an Interior Gateway Protocol (IGP). IGP is a routing protocol for transferring information between routers in a single system. IGP has two main types: Distance-vector routing protocol and Link-state routing protocol. The difference of the two types is that in Link-state routing protocol each link has an identical database which has the information of the systems topology. With that information, each link calculates which next hop is the most suitable for it. Only IGP communication between the links are flooded messages of the links updated states. In Distance-vector routing protocol the links have an individual routing table which they update based on the information they get from the adjacent links. The information is called advertisements and they hold distance and direction vectors of the link. There are multiple protocols of each type and some of them are explained more in chapter 5. [45]

As mentioned earlier the PWE3 doesn't provide any security measurements for the transferred packets. Additional security protocols can be utilized to improve security and one possible solution is MAC Security (MACSec), which is explained further in chapter 5.2.1. IPsec on the other hand cannot be used in EoMPLS solutions because of the label form of the packets. IPSec requires that the encapsulated packet has an IP packet header. Security protocols are further introduced later in chapter 5.2. For resiliency, the options are similar to L2TPv3 due to the reason they both use PWE3 pseudowire.

4.1.3 Generic Routing Encapsulation

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems. It offers packet encapsulation and tunneling over layer 3 IP network. The GRE is a hardware relying protocol and it requires routers that support it. The transmitted packets are encapsulated into GRE packets with a specific 4 octet GRE header. In addition to adding the GRE header the packet is also encapsulated in a 20 octet IP header. There are two different types of the GRE encapsulation which can be used: [46] and [47]. The main difference between the two is the GRE packet header form. It can be said, that the 2784 form is the standard today, but the 1701 form is still used and supported by some switches. The structures of the two GRE encapsulation forms can be seen in figure 17. After a received packet is encapsulated with GRE header, it is then transferred through a point-to-point tunnel that is created between two end routers. GRE can transfer multicast messages what a regular IP packet can't do. It supports multiple Layer 2 and Layer 3 protocols and can be used to transfer other tunnel protocols such as L2TPv3 and MPLS. [48]

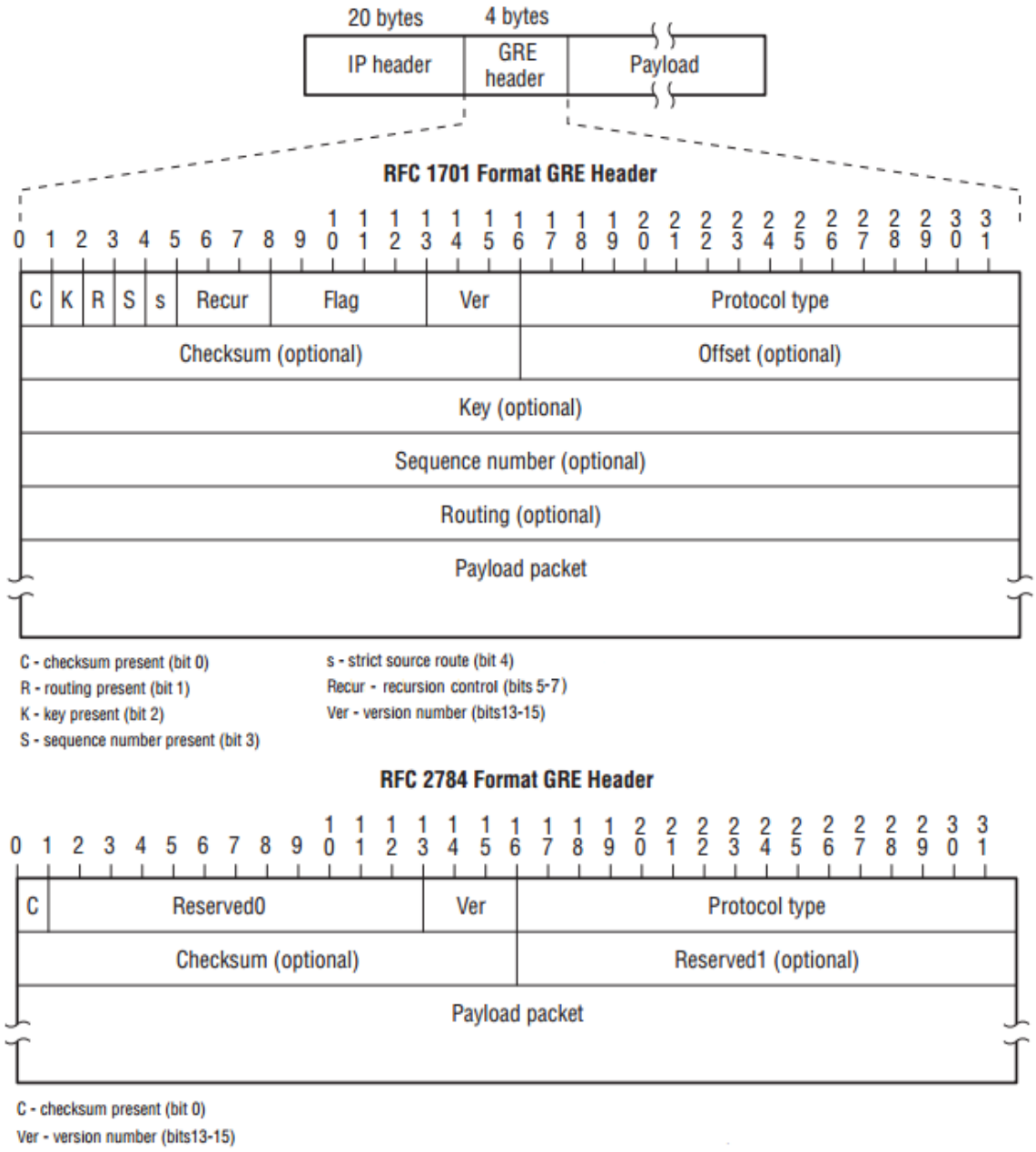


Figure 17 GRE packet structure, RFC 1701 and RFC 2784. Original figure from [42]

Constructing a GRE tunnel is simpler than with other tunneling protocols. The tunnel is constructed using the existing routing tablets of 2 PE routers. Because the top header is a normal IP header the packets are handled as such. The benefit of GRE is that it can transfer multicast and broadcast packets in addition to unicast packets. It can also transfer multiple protocols over IP, even non-IP based protocols like MPLS. GRE also supports VPN over the network. On the downside, GRE doesn't provide any encryption for the encapsulated packet and therefore a separate security protocol should be used if data protection is needed. For network layer one possible choice is IPSec and it is explained later in Chapter 5.2.2. [48][47]

4.1.4 Not studied protocols

Point-to-Point Tunneling Protocol is an old VPN tunneling protocol which is used to tunnel Point-to-Point Protocol traffic. It has many serious security issues and vulnerabilities and is now considered as an obsolete protocol. [49]

Secure Socket Tunneling Protocol is a VPN tunneling protocol which uses TLS/ Secure Sockets Layer to form the tunnel and for authentication. The SSTP is only able to transfer Point-to-Point Protocol traffic and is therefore not included into to this study. [50]

OpenVPN is on open source application which provides a point-to-point VPN tunnel. Because it requires a software, that is free, to be installed on both end-point devices it is not included into to this study, although some routers have it already built-in.

5. NETWORK FAULT MANAGEMENT AND SECURITY

In this chapter, protocols and methods used to make an automation system more reliable are studied. This includes looking closer to fault control methods and security protocols.

The most important features in automation system security are integrity, confidentiality, accountability and availability. Integrity means that data is protected with authentication techniques. This means securing the data with password authentication or key based cryptography. Also, devices that are allowed to access the network can to be authenticated with specific certificates. Confidentiality means that the data is encrypted to prevent easy comprehension if it gets into wrong hands. Some communication protocols have built-in data encryption and also separate security protocols for different network layers can be used. Accountability means that the communication can be checked later if needed. This includes timestamps in messages and storing data to some extent. Availability means that data should always be available and connection breaks minimized. Automatic constant monitoring of connection states with alarms can reduce the down time drastically. Addition to connection breaks also traffic overload causes disturbance in availability and can make the system to fail the set message time requirements. Data availability can be improved by using by using redundancy techniques like different network topologies and protocols. [11][42]

5.1 Fault control and redundancy

Modern communication networks are becoming faster, more complex and need to offer steady data flow, good safety and resilient connections. A quick recovery when a link failure occurs is becoming a mandatory requirement. Even a short loss of connectivity can cause damage to the network, to devices in the network and in some cases, even to the personnel working with devices connected to the network [51]. Redundancy in a network can be divided into three areas:

- Hardware redundancy
- Link redundancy
- Path redundancy

There are multiple link and path redundancy protocols and supporting techniques available and selected few are introduced in this chapter. Also, two hardware redundancy protocols are introduced.

5.1.1 Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a lightweight protocol that is used to detect faults in a path between two forwarding engines, but also communication failures in data links. The fault detection is based in simple cyclical Hello messages that are sent periodically from one end to the other. When a 'Hello' is not received in a certain time window the connection is declared as broken. The BFD can be used on any data protocol, so it suitable for network layer, data link layer and also tunnels. The used communication mode is point-to point and the messages are always sent in unicast mode. Also, multiple BFD sessions are supported and they can be constructed for each path between the end points. Due to being a very light protocol, the impact of BFD to the router strain is minimal.

A BFD session is established and taken down using a three ways handshake. The time how long Hello messages are waited, is estimated by each system and agreed with adjacent devices. This way the time is different between each device and supports devices with different processing speeds. The message encapsulation and transfer method depends on the protocol which uses BFD. The protocol has two operation modes: Asynchronous mode and Demand mode. Asynchronous mode is the default mode in which devices send Hello messages periodically. In Demand mode, an end point can inform the other end to set the sending of Hello messages to a halt. This does not affect a specific connectivity checks that the BFD sends. To provide additional protection to the BFD, an authentication section may be added to the messages. [52][53]

5.1.2 Link Aggregation Group

Link Aggregation Group (LAG) is a technique that protects from circuit failures. LAG works by combining multiple physical links and treating them as a single logical link. The benefit in this is that if a single physical link fails the traffic is forwarded to the other working links inside the LAG logical link. LAG provides resilience to links and improves availability of the whole system. If multiple nodes are connected to a single LAG endpoint, the connections can be aggregated using Multi-Chassis LAG (MC-LAG). By using MC-LAG redundancy can be extended for node level also. The LAG forms an additional sublayer in OSI model's data link layer, between the LLC and MAC layers, as seen in Figure 2. [53]

Addition to providing resilience to the system, there are several other benefits that are gained with LAG. First, the bandwidth is increased due to multiple connections. Also, in LAG it is possible to divide traffic evenly between the aggregated connections, which reduces bottlenecks what a single connection might cause. Also, LAG doesn't cause any changes to the standard 802.3 Ethernet frames, so it doesn't increase the frame size either. [54]

5.1.3 Open Shortest Path First

Open Shortest Path First (OSPF) is a protocol of the routing Interior Gateway Protocol. The main purpose of OSPF is to calculate shortest routes between routers, which provides faster routing of the packets. It also prevents that the routes don't form loops in the network. OSPF works in network layer of the OSI model and it's designed especially for IP networks. It is a link-state type IGP, which means that each link has an identical database of the network topology and they calculate the next hop using that. Each link broadcasts its state with an update message to other links when it is updated. A single router may belong to multiple OSPF areas and have a separate database and calculation algorithm for each of them. The received packets are routed based on the IP address of the packet header. OSPF doesn't alter the packets in any way. [45]

OSPF routers identify their neighbors with Hello messages which are sent when the routers are started. In broadcast networks, the Hello messages and other protocol packets are broadcasted using a defined 'AllSPFRouters' multicast address 224.0.0.5. The transmitted data is directly encapsulated in IP packets, so TCP or UDP packets are not utilized. The OSPF messages include: Hello, Database Description, Link State Description, Link State Update and Link State Ack messages. The Link State Update messages, that are also called advertisements, update the state in other routers. All OPSF messages, except Hello messages, are only sent to adjacent routers which then sent the information forward in their messages. The messages in OPSF are authenticated with a 64-bit authentication data field which is in the header of each message. There are 3 authentication types: null authentication, simple authentication and cryptographic authentication. The authentication is defined with a separate field in the OSPF header. [45]

5.1.4 Virtual Circuit Connectivity Verification

Virtual Circuit Connectivity Verification is an IETF standard that provides a control channel for pseudowires. The control channel is built between the tunneling protocols endpoints, or Provider Edges (PE), and its functions are end-to-end fault detection and diagnostics mechanisms. The VCCV follows the PWE3 protocol stack and it is usable with both L2TPv3 and EoMPLS tunneling protocols. The VCCV messages are encapsulated using PWE3, but the structure varies regarding which tunneling protocol is used. The VCCV is set up at the same time as the pseudowire is constructed and the configuration information is included into the pseudowire signaling messages. The initial information includes the Control Channel and Connectivity Verification types. The VCCV offers both fault detection and diagnostic operations for the underlying pseudowire. The operation activation can be automatic and set to start periodically or they can be manually activated when needed. Activating the VCCV operation starts one Control Channel and one Connectivity Verification type functionality. The Connectivity

Verification consist of ping operation and Control Channel defines the channel type in which the Connectivity Verification is transferred. [55]

BFD can be used with VCCV to provide additional Connectivity Verification types. The new types improve the pseudowire state monitoring and better signaling options. The BFD messages are sent using the VCCV Control Channel, so additional control channel is not needed. Two encapsulation techniques can be used: UDP encapsulation, which includes a UDP header, and a direct VCCV encapsulation, which doesn't use any additional headers. It should be noted that with VCCV only one BFD session can be established per pseudowire. [41]

5.1.5 Parallel Redundancy Protocol

Parallel Redundancy Protocol (PRP) is a redundancy protocol standardized in the IEC 62439-3. It offers a zero-time recovery for layer 2 Ethernet networks. PRP is designed for most Industrial Ethernet protocols but it is also usable with IEC 61850. The concept of PRP is that two parallel LANs are created and the used devices are connected to both of them. The LANs must be completely separate so that they are fail-independent. Devices using PRP are called Doubly Attached Node with PRP nodes and both LANs must be connected to separate Ethernet ports. The PRP nodes duplicate each message and sends one to each LAN simultaneously. The duplicated messages are identified with an additional Redundancy Control Trailer field added to the transferred Ethernet frames. In case of a failure in one LAN, the other LAN continues without disturbances. With this method, the zero-time recovery is possible. Down side of PRP is that it doesn't provide end node redundancy. Also, the construction costs are doubled as two LANs with own devices are required. [9][56][57]

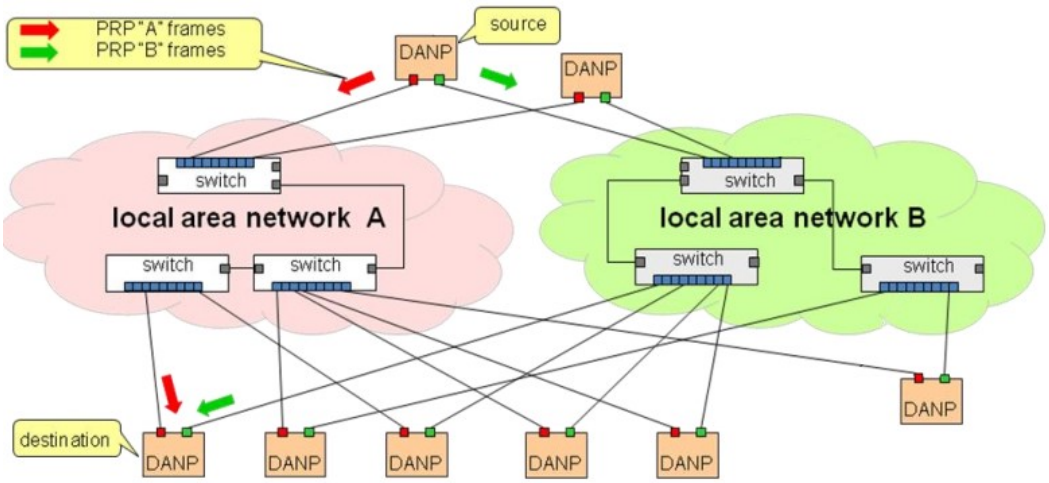


Figure 18 PRP architecture example. Original image from [9].

5.1.6 High Availability Seamless Redundancy Protocol

High Availability Seamless Redundancy Protocol (HSR) is a redundancy protocol standardized in the IEC 62439-3. PRP and HSR have some similarities but use different redundancy methods. Same way as PRP, HSR also offers a zero-time recovery for layer 2 Ethernet networks. HSR is also designed for most Industrial Ethernet protocols and also with IEC 61850. In HRS, the redundancy is constructed using a ring topology and each device is connected to the ring with two Ethernet ports. The HSR devices are called Doubly Attached Node implementing HSR nodes and they also duplicate each message and sends one to each Ethernet port simultaneously. This makes the messages to travel in the ring and finally end up back in the sender device if they didn't reach the destination device. Each device along the ring reads and passes the messages on. The duplicated messages cause the destination device to receive the same message twice and it must discard the second one. The duplicated messages are identified with an additional HSR Tag added to the transferred Ethernet frames. In case of a failure at one part of the ring, the messages can still reach each device in the ring. It is also possible to connect multiple rings to each other using Quadboxes. A Quadbox has four Ethernet ports which are linked together inside the device. Additional redundancy can be added by using two Quadboxed, so that the 2-ring network can continue to work without disturbances even if one Quadbox fails. [9][56]

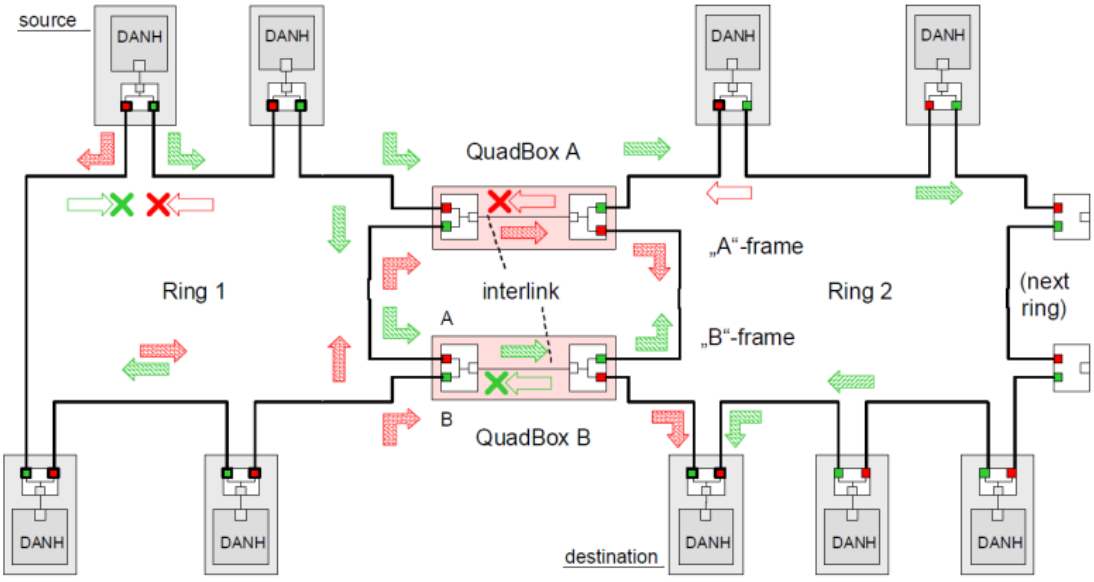


Figure 19 HSR topology example. Original image from [9].

5.2 Security

The OSI model is designed so that the different layers work without knowledge of each other. A benefit in this is that protocols on different layers won't affect each other's functionality. A negative side of this is that if security on one of the layer is compro-

mised, it has no means to inform other layers about it [56]. What this means, is that the used OSI layers should have at least some protection. In this thesis, security is limited to layer 2 Ethernet tunneling operations, meaning that the focus is only in data link layer and network layer security protocols that are compatible with the tunneling protocols presented in Chapter 4. Higher level, like application level security protocols are outside the scope of this thesis. As seen in Chapter 3, some communication protocols have built-in security measurements, but they are not addressed in this chapter. The built-in security might not be enough to meet today's requirements, so the recommended solution would be to combine several security protocols to reach the wanted protection level. The solutions explained here are open solution with no restrictions to certain manufacturers devices or licenses.

5.2.1 Media Access Control Security

Media Access Control Security protocol is a layer 2 security model and it is an IEEE security standard 802.1AE. First edition of the standard was published in 2006 and latest version is from 2013. It provides security between point-to-point Ethernet links, but doesn't provide end to end security across public networks and therefore a higher layer security solution, like IPSec, is recommended to be used with MACSec. In general, MACSec is a simple security protocol to implement and provides data confidentiality, integrity and authenticity. [59]

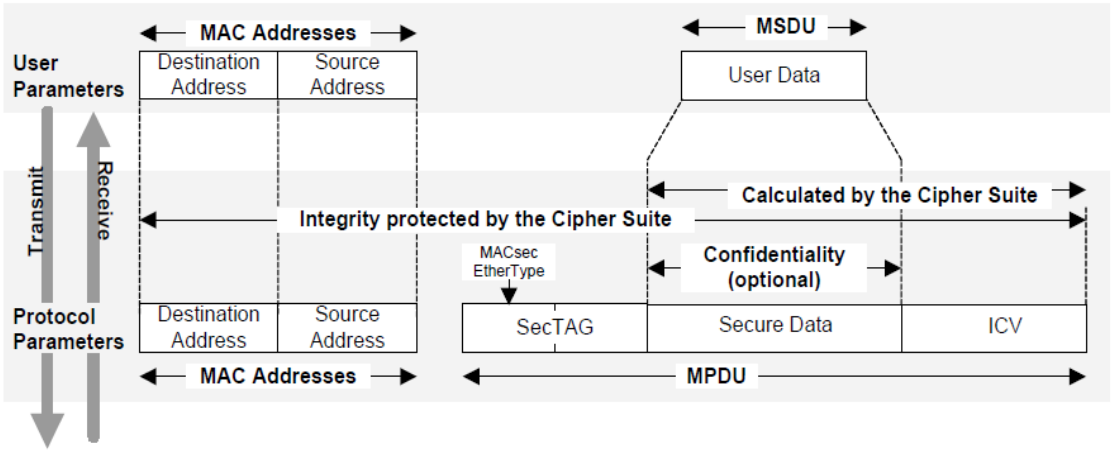


Figure 20 Structure of a MPDU [59]

MACSec provides data confidentiality, data origin authentication, message replay protection and data integrity in a LAN where it is implemented. MACSec works by creating a Connectivity Association between the stations in LAN that are using MACSec. The stations also form unidirectional point-to-multipoint Secure Channels between each other. The security is provided with the use of MACSec frames called MACSec-Protocol Data Units (MPDU). The MPDU is a variation of the Ethernet frame with additional fields. The MAC destination and source address fields are in the beginning the

MPDU frame. A comparison between the structure of MPDU and the normal MAC service data unit (MSDU) is shown in Figure 20. The MPDU data consist of three fields: SecTAG (8 or 16 octets), Secure data (0 to n octets) and Integrity Check Value (8 to 16 octets). The fields inside SecTAG are shown in Figure 21. Stations forming a MACSec CA can also function like normal stations and receive non-secure Ethernet frames from devices not using MACSec. [60]

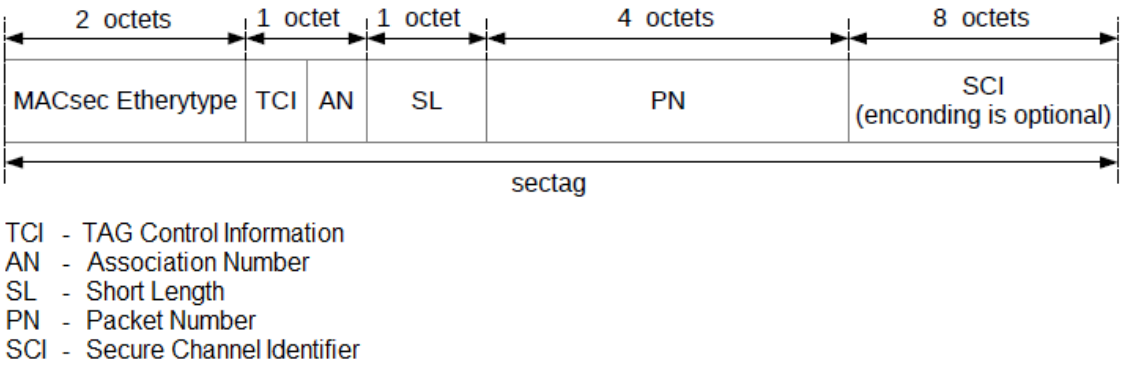


Figure 21 MACSec SegTAG structure [59]

In each station, a MAC Security Entity handles the transferring and receiving of packets. The Security Entity doesn't know about the other stations in the Connectivity Association, it is only aware of the Secure Channels. In each station, there is also a MACSec Key Agreement Entity that handles the stations authentication and authorization procedures and also the discovering of other stations inside the Connectivity Association. Key Agreement Entity is a IEEE 802.1AF standard which is designed solely for MACSec. The authentication of each device is confirmed with symmetric keys. The default cryptography cipher suite used in the keys is symmetric GCM-AES-128 (Galois/Counter Mode of Advanced Encryption Standard) cipher with 128 bit key. In 2011 MACSec was updated with a possibility to use ciphers using AES-256, which uses 256 bit keys. The protection that MACSec provides is: data origin authentication, confidentiality replay protection and connectionless data integrity. Also, it lowers the success rate of Denial of Service (DoS) attacks, but can't provide full protection against them. [59][56]

5.2.2 IP Security protocol

IP Security (IPSec) protocol is an open layer 3 security protocol that provides high quality cryptography based end-to-end security for IP-based communication protocols. IPSec can be used also as layer 3 tunneling protocol, which is called Tunneling Mode, in addition to using its security functions, which is called Transport Mode. It has support for both IPv4 and IPv6 protocols and is designed to be interoperable with multiple systems. IPSec provides protection only to layer 3 and above layers, meaning the it provides protection only to the tunneling protocol and tunnel part of the system. The IPSec

defines 2 different protocol: Authentication Header (AH) and Encapsulating Security Payload (ESP). Both of the protocols have a tunneling mode for full data encapsulation, but it is optional and only the security features of the protocols can be utilized.

The AH protocol provides authentication services for the IP packets. It doesn't encrypt the data, but adds an authentication header that provides data integrity. It also protects the address fields and provides data origin authentication and replay detection. On the other hand, AH doesn't provide data confidentiality and an additional protection method should be used in systems where it is required. One option is to combine AH with the ESP protocol. For authentication, possible algorithms are either MD5 (Message Digest) or SHA-1 (Secure Hash Algorithm). [61][62]

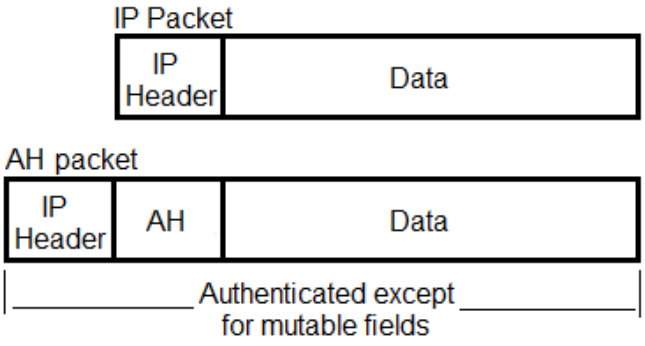


Figure 22 IPSec AH structure [62]

The ESP protocol can provide data integrity, confidentiality, replay detection and data origin authentication for IP packet. With ESP, it is possible to use both encryption and authentication security for an IP packet and the security services vary depending on how the ESP is implemented. For encryption, 3 symmetric algorithms can be used: Data Encryption Standard (DES), Triple DES (3DES) or Advanced Encryption Standard (AES). From asymmetric algorithms only RSA is supported. For authentication, possible algorithms are either MD5 or SHA-1. [61]

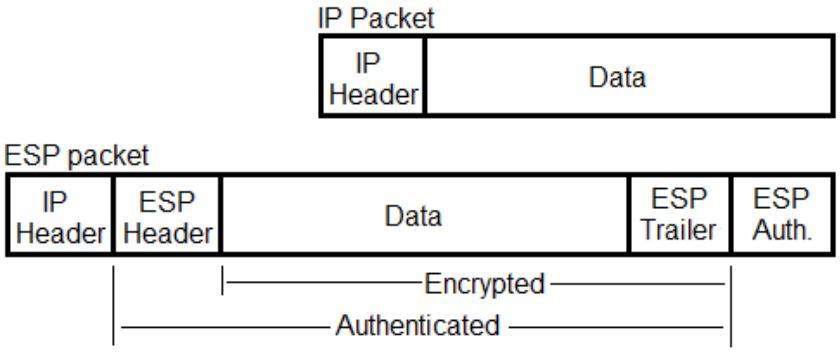


Figure 23 IPSec ESP structure [62]

IPSec uses an authentication key based security with encryption. The security agreement of the IPSec end points is created using a Security Association, which defines the

used algorithms and parameters. The actual key management used in the Security Association is called Internet Security Association Key Management Protocol. It creates a channel for dynamic agreement between end points on the used Security Association before any data communication is allowed. The keys are generated using an Internet Key Exchange (IKE) protocol. It also handles the exchange of the security parameters using the Security Association. [62][56]

6. LAYER 2 COMMUNICATION TUNNELING SOLUTIONS

In this chapter, potential ways to construct layer 2 Ethernet communication tunneling solution are inspected. The solutions are build using the methods and protocols presented in the previous chapters. Spectrum of systems where layer 2 tunneling can be used is vast and they each have specific requirements and suitable solutions. In this thesis solutions are inspected using two use cases:

- Coordinated voltage control
- Automated fault isolation and recovery

Looking at the presented methods and protocols from the previous chapters, without going into performance details, interoperability between them is fairly broad. All three tunneling protocols can be used with each of the presented communication protocols. As for security, L2TPv3 and GRE can use both IPSec and MACSec protocols. With EoMPLS only MACSec can be utilized, because IPSec is not compatible with the label encapsulation that EoMPLS uses. A solution for this would be to tunnel EoMPLS inside GRE, and then apply IPSec. In resilience methods and redundancy protocols there is a larger variation due to the difference in tunneling methods. L2TPv3 and EoMPLS uses a pseudowire tunnel, which limits the resiliency choices. GRE, on the other hand, just utilizes a virtual tunnel between two routers, so it has the same features as a normal IP network.

6.1 Use case 1: coordinated voltage control

This use case concentrates in low voltage area of a power distribution network. Coordinated voltage control (CVC) is an active method of controlling voltage levels in a distribution network. The method is based on automated voltage control relays which control the on-load tap changers using calculations that are done in real-time using selected algorithms. CVC is especially useful in modern networks where distributed generators are also present. First problem in these networks is that the power can flow in both direction, in to the network and out to the upper level network, depending on the consumption and amount of generated power. Another reason is that the power generated by a distributed generator unit, for example photovoltaic generators or wind turbines, can vary greatly in a short time depending on external conditions. Distribution networks are commonly controlled using a SCADA system. SCADA is a control and monitoring system that can be implemented to cover the whole distribution network. SCADA is

usually divided into multiple sections which work independently but can be controlled from higher level if needed. Details of SCADA systems are not included in this thesis but they give a good reference of what type of communication methods are used in the MV/LV grids. An example of a LV grid CVC architecture can be seen in Figure 24. The CVC unit is physically located inside the substation. The figure is from a European Commission funded project called IDE4L (Ideal Grid for All) that studied active electrical distribution networks also substation automation units. [63][64]

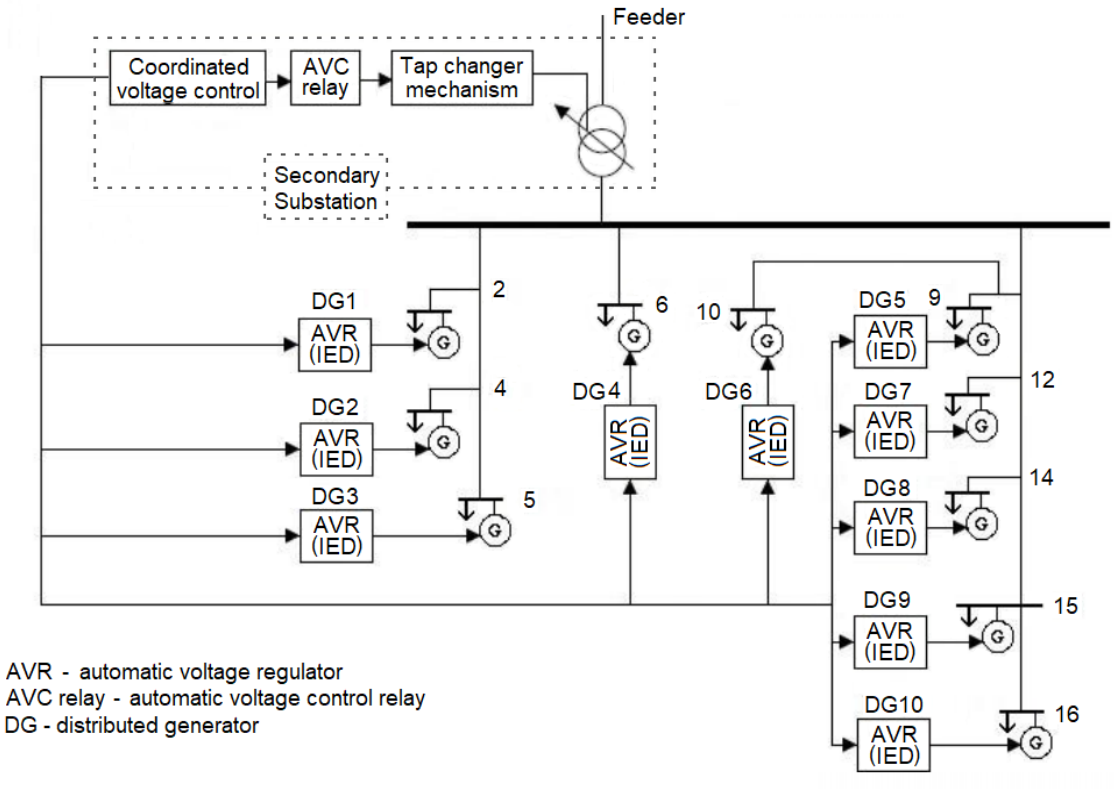


Figure 24 Low Voltage area control architecture [65]

The layer 2 tunneling is implemented to enable communication between secondary substations (SS) and IEDs, and additionally communication between IEDs. The LV grid communication principle is that SS gathers information from the IEDs and communicates with a primary substation, which sends control messages back to SS. By adding intelligence to SS's, they can get the needed information about the networks state from the IEDs and make control actions themselves. This speeds up the control process and helps to solve fault situations faster. Communication between IEDs can be used as an additional communication route for example if a failure occurs in IEDs connection to the SS. Figure 25 shows the communication design. Requirements for the voltage control tunneled communication are:

- Soft real-time communication. For external substation communication, [66] gives 1 second requirement for monitoring and control information.
- Data encryption and authentication.

- Resilient connection with automatic condition and fault checks.

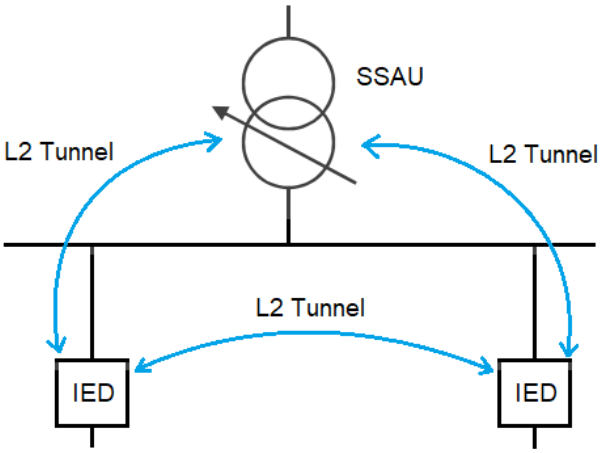


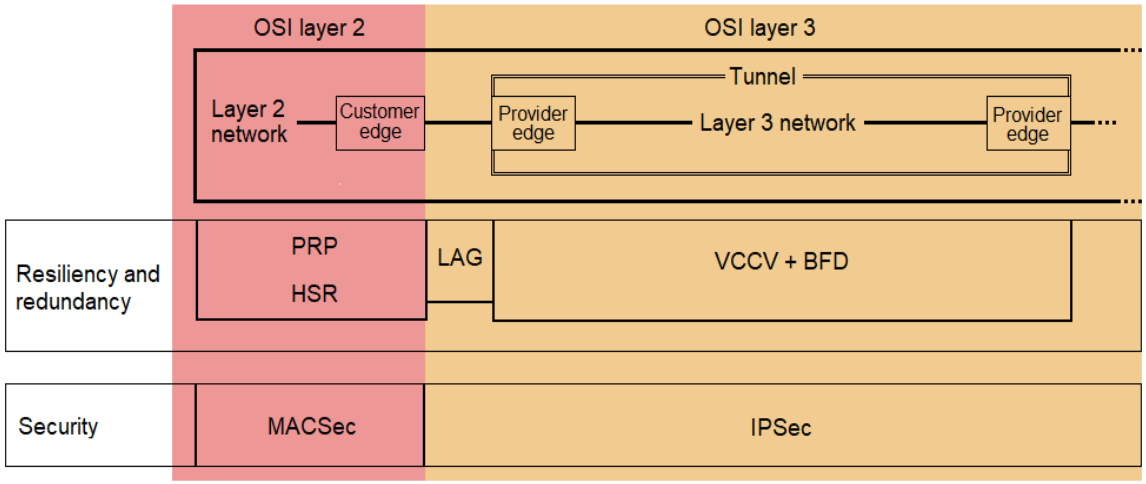
Figure 25 Use case 1 communication design

A suitable communication protocol depends much what protocols are supported by the IEDs. If looking at SCADA substation protocols, the most commonly used are: IEC 60870-5-104, DNP3, Modbus/TCP and IEC 61850 [11][64][67]. From these Modbus/TCP has disadvantage because in it all communication must be requested by the client side. This makes it difficult to send for example alarms from the server side. The other three are all suitable protocols and can manage real-time communication. IEC 61850 GOOSE and SV protocols have a benefit of being directly mapped on top of Ethernet. DNP3 and IEC 60870-5-104 are higher level protocols but utilize Ethernet in data link layer. All three protocols can use a security features defined by IEC 62351 standard to add additional application level security. From the mentioned protocols IEC 61850 GOOSE is gaining more popularity among new systems and it is also developed and innovated constantly [68][69], so it is the recommended communication protocol.

The tunneling protocol should be chosen based on what layer 3 network is used. In case of MPLS network EoMPLS should be used, and if IP network is used, either L2TPv3 or GRE tunneling protocols should be chosen. Alternative option is to use EoMPLS and encapsulate it with GRE to be able transfer it over IP network. This however makes things more complicated and adds additional things that can have faults. Speed difference between L2TPv3 and EoMPSL is not significant [70]. GRE provides a multipoint tunnel and the other two a point-to-point tunnel. For security MACSec can and should be used to provide protection on layer 2. With MACSec the layer 2 gets data integrity, confidentiality and origin authentication. In layer 3, on top of tunneling protocol, IPSec should be used. It provides end-to-end security over network layer with authentication and/or encryption. As mentioned earlier IPSec cannot be used with EoMPLS unless it is first encapsulated with GRE protocol and transferred over IP network. Using multiple encapsulations causes the packet header size to grow and it result in packet fragmenta-

tion. To avoid fragmentation the maximum transmission unit (MTU) size should be reduced, which also affects negatively to the data transfer rate.

To make the tunneling solution resilient and redundant, the selectable options vary depending on which tunneling protocol is chosen. Figure 26 shows what areas of the system different protocols and methods affect and how they are located in the OSI model. To provide redundancy, the tunneling protocols should at least have at least one secondary connection. The connections can use the same or separate PE devices. Also, connections from Customer Edges (CE) to Provider Edges (PE) should have a secondary line. By using LAG these CE-to-PE lines can be combined to protect from failures. With multiple PEs and/or CEs, the MC-LAG can be used alternatively. To ensure tunnel resilience, if pseudowire tunneling protocol is used, VCCV should be utilized for end-to-end fault detection. The VCCV requires a separate method to detect the faults, and the BFD can be used for that. With L2TPv3 methods provided in the failover extension [40] can be used. Of course, in layer 2 also the HSR and PRP protocols provide faster failover recovery although it doesn't add redundancy for the actual tunnel. The communication can be transferred over network layer using physical or wireless connection. Key factors of choosing the right transfer medium is the distance of communicating devices, budget and the required speed for the data transfer.



PRP - paraller redundancy protocol
HSR - high availability seamless redundancy protocol
LAG - link aggregation group
VCCV - virtual circuit connectivity verification
BFD - bidirectional forwarding detection
MACSec - MAC security
IPSec - IP security

Figure 26 Use case 1 solution breakdown

6.2 Use case 2: Automated fault isolation and recovery

This use case addresses automated fault isolation and recovery. Today more intelligence is added to the automation systems to give the devices more functionalities and make

them more autonomous. Fault control is an important part that should be implemented to every system. By having an automated fault control, devices and their operations can be shut down, areas or devices can be isolated and recovery can be initiated by the system itself. This does not only make the devices safer to use, but also increases the protection in the whole system. In automated fault isolation and recovery functionalities fast communication plays a vital role, and therefore hard real-time communication is set as a requirement in this use case.

The studied environment is a networked control system (NCS). An NCS is a system where devices communicate with each other over a shared network. The main difference between a traditional, directly linked, control system is that devices are connected to a common network and can communicate even from long distances. Devices that are commonly used in NCS's are controllers, actuators and sensors. An example of an NCS is presented in Figure 27. An NCS can be implemented in multiple different applications, like industrial and manufacturing automation, smart grids and power distribution systems. The benefits of NCS is its low implementation cost, easy maintenance, flexibility and minimal wiring. [71] [72]

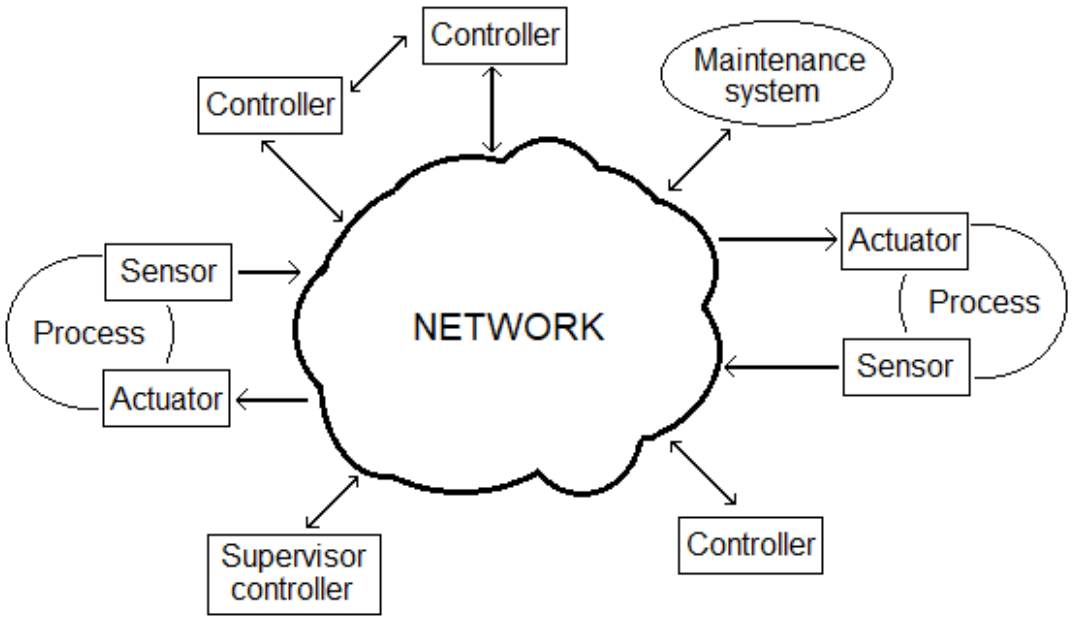


Figure 27 Example of a network control system architecture

The goal in this use case is to study hard real-time communication over the shared network using Ethernet communication and tunneling protocols. The focus is on the communication between controllers and process devices. The process devices can be anything from sensors and actuators to motors. The controllers can be part of a SCADA system, programmable controllers or some other type of controllers. The shared network varies depending on the system and it can be for example a Fieldbus, wireless, Ethernet,

control area network (CAN), MPLS or IP network. In this use case, the network is a MPLS or IP layer 3 network. The devices and controllers must utilize layer 2 and Ethernet communication. Regarding Ethernet protocols, process automation systems commonly use Industrial Ethernet protocols which are more suitable for industrial environments. Requirements for the tunneled automated fault isolation and recovery communication are: [71]]72]

- Real-time communication. Because this tunneling solution can be used in substation automation, 8-12 millisecond time requirement for protection communication can be taken from [66].
- Data encryption and authentication.
- Resilient connection with automatic condition and fault checks.

In industrial automation systems, Industrial Ethernet protocols are often used. From the Industrial Ethernet protocols introduced in this thesis, PROFINET and Ethernet/IP could be chosen. Modbus/TCP has a disadvantage because of its client-side polling method, which is not suitable when fast alarms from server side are required. DNP3 and also IEC 61850 GOOSE and SV modes can be used, although they are primarily designed for substation communication they can be utilized in other automation systems also [73]. The tunneling protocol should be chosen based on what layer 3 network is used. In case of MPLS network EoMPLS should be used, and if IP network is used, either L2TPv3 or GRE tunneling protocols should be chosen. Alternative option is to use EoMPLS and encapsulate it with GRE to be able transfer it over IP network. This can make the process slower due to multiple encapsulations. The speed difference between L2TPv3 and EoMPSL is not significant [70], but additional GRE encapsulation can slow the EoMPLS down. Benefit of GRE is that it provides a multipoint tunnel and the other 2 only a point-to-point tunnel. For layer 2 security MACSec should be used to provide data integrity, confidentiality and origin authentication. For layer 3 security IPSec should be used to provide end-to-end security over network layer with authentication and/or encryption. With IEC 61850, additional application level security features can be gained by utilizing IEC 62351 standard.

For making the tunnel resilient and redundant, the same solutions as in use case 1 apply also in this case. And as before, the selectable options vary depending on which tunneling protocol is chosen. In Figure 28, the different protocols and methods OSI model positions are shown, and also which part in the system they affect. At least one secondary tunnel connection should be constructed to provide redundancy. The connections can use the same or separate Provider Edges (PE) devices. Additionally, connections from Customer Edges (CE) to PE should have at least one secondary line. By using LAG these CE-to-PE lines can be aggregated to protect the communication from failures. Alternatively, if multiple PEs and/or CEs are used, MC-LAG can be implemented. In pseudowire tunneling protocols, VCCV should be utilized for end-to-end fault detection to ensure resilient connection. A separate fault detection protocol can be used with

VCCV, and the BFD can be used for that. As a lightweight protocol, BFD doesn't cause extra load in the tunnel. If L2TPv3 tunneling protocol is selected redundancy methods explained in the failover extension [40] can be used. Additionally, the HSR and PRP protocols can be implemented for faster failover recovery. It should be noted that they only affect layer 2 and doesn't add redundancy for the actual tunnel. The communication can be transferred over network layer using physical or wireless technology. If physical technology is used, fiber is the best solution for its speed advantage compared to other technologies.

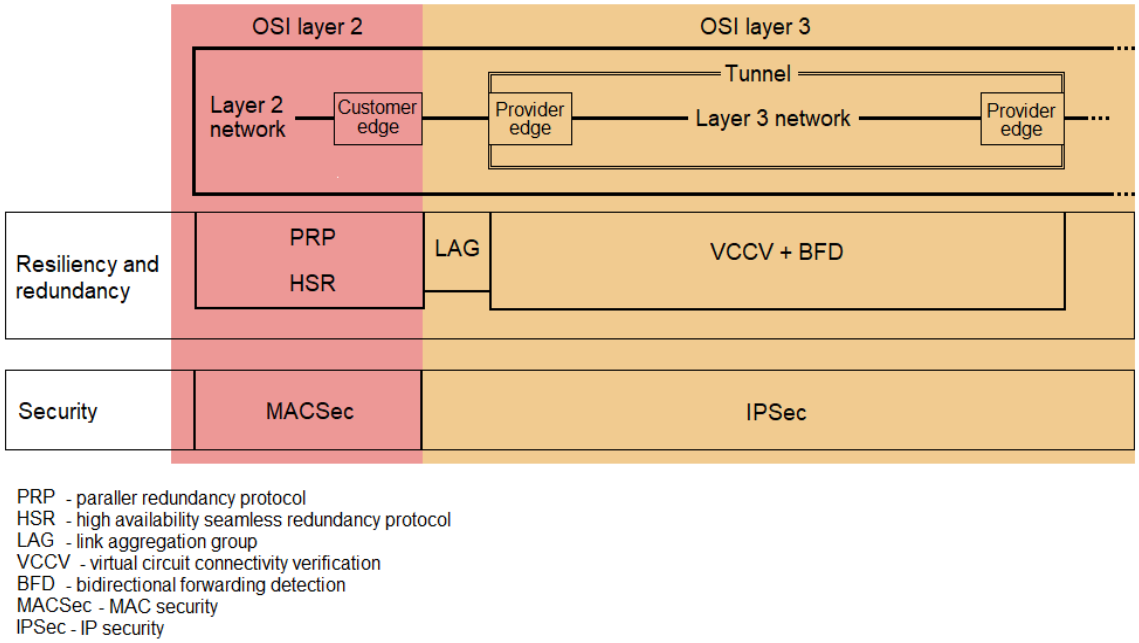


Figure 28 Use case 2 solution layer breakdown

7. CONCLUSION

The goal of this thesis was to study and provide information about layer 2 Ethernet communication tunneling possibilities. The purpose of Ethernet communication tunneling is to provide a method for achieving real-time communication over network layer. Tunneling protocols create a direct connection between network end-points making the routing of packets much simpler and faster than it is for example with regular IP routing. Tunneling protocols also handle packet encapsulation and de-capsulation allowing non-routable protocols to be transported over higher level networks. The focus in the study was in automation systems in general, with additional attention given to energy distribution networks and smart grids. Layer 2 communication tunneling is not widely utilized feature even though the technology has been available for a long time. One goal of this thesis is to provide information to those who are not aware or only know only a little of this technology.

Before the possible solutions were studied, components needed for the solutions were presented. At first, suitable communication and tunneling protocols were introduced, followed by resilience and redundancy technologies. Lastly, applicable layer 2 and layer 3 security protocols for tunneling protocols were presented. Finally, possible Ethernet communication tunneling solution were studied using two use cases. The first use case concentrated in coordinated voltage control in power distribution networks low voltage areas. The second use case studied automated fault isolation and recovery in networked control system.

The layer 2 tunneling solutions for both use cases were quite similar due to the wide suitability of the protocols and solutions. Also, because this thesis didn't have any actual tests, no exact answers were given. With the proposed solutions and information provided in this thesis, it should be easier to choose a suitable tunneling protocol and other technologies for a planned system.

7.1 Future studies

A clear follow-up for this thesis is to make actual tests using the provided information. Also, additional use cases with larger variety of environments and equipment could be inspected. As the Internet of Things (IOT) is developing and popularizing, it would be interesting to see what kind of tunneling solutions could be implemented with that technology and how the requirements of IOT can be fulfilled. Also, 5G as another new technology brings low, power wide-area networks, low latency and high data rate features to wireless communication.

REFERENCES

[1] J. D. McDonald, B. Wojszczyk, B. Flynn, I. Voloh, Distribution Systems, Subsystems and Integration of Distributed Generation, in: M.M. Begovic (ed.), Encyclopedia of Sustainability Science and Technology, 2013, pp. 7-69

[2] R. Silvola, Reaaliaikaiset teollisuus-Ethernet -ratkaisut automaatiojärjestelmissä, Master of Science Thesis, Tampere University of Technology, August 2006, pp 98, Available: http://ae.ase.tut.fi/research/AIN/Publications/ThesisSilvola2006.pdf

[3] A.P. Bowen, C.H.R. de Oliveira, IEC 61850 GOOSE Message over WAN, Proceedings of the International Conference on Wireless Networks (ICWN), 2012, pp. 3.

[4] CLIC, FLEXE – FUTURE FLEXIBLE ENERGY SYSTEMS, Clic Innovation, Webpage. Available: http://clicinnovation.fi/activity/flexe/ [Accessed: 6.7.2016]

[5] W. Cui, D. Li, Y. Li, R. Zhang, Research based on OSI model, Communication Software and Networks (ICCSN), IEEE 3rd International Conference, Xi'an, China, May 2011, pp. 4

[6] S. Tunis, Real-time industrial Ethernet in machine automation systems, Master of Science Thesis, Tampere University of Technology, December 2009, pp. 82, Available: https://dspace.cc.tut.fi/dpub/handle/123456789/6592

[7] A. Altaher, S. Mocanu, J.-M. Thiriet, Evaluation of Time-Critical Communications for IEC 61850-Substation Network Architecture, Surveillance 8 International Conference, Roanne, France, October, 2015, pp. 8, Available: https://hal.archives-ouvertes.fr/hal-01242297

[8] D. Dolezilek, V. Skendzic, D. Whitehead, Integration of IEC 61850 GSE and Sampled Value Services to Reduce Substation Wiring, 47th Annual Minnesota Power Systems Conference, Brooklyn Center, Minnesota, November 1–3, 201, pp. 6.

[9] M. Taikina-aho, Redundant IEC 61850 communication protocols in substation automation, Master of Science Thesis, University of Vaasa, 2011, pp. 133, Available: http://www.tritonia.fi/?d=244&g=abstract&abs=4594

[10] M.A. Gallo, W.M. Hancock, Data Link Layer Concepts and IEEE Standards, Networking Explained, Second Edition, Digital Press, December 14, 2001, pp. 181-212

[11] P. Jafary, H. Koivisto, S. Repo, Secure Communication of Smart Metering Data in the Smart Grid Secondary Substation, IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA), 2015, pp. 7.

[12] ExtremeXOS 15.5 User Guide, Extreme Networks, 2014, pp. 323, Available: [extrcdn.extremenetworks.com/wp-content/uploads/2014/04/Layer_2_Protocols.pdf]

[13] N. Higgins, N.-K.C. Nair, K. Schwarz, V. Vyatkin, Distributed Power System Automation With IEC 61850, IEC 61499, and Intelligent Control, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), Volume 41, Issue 1, 2011, pp. 81-92.

[14] J. Piirainen, Applications of Horizontal Communication in Industrial Power Networks, Master of Science Thesis, Tampere University of Technology, May 2010, pp 62, Available: https://dspace.cc.tut.fi/dpub/handle/123456789/6601

[15] D. Boeda, P. Coudray, I.M.D. de Cerio, D. Eckardt, H. Elias, M. Ferdowsi, P. Goergens, J. Heiles, C.H. Jensen, H. Jormakka, D. Koziol, M. Kranich, T. Kyntäjä, J. Liu, Y. Pignolet, M. Wagner, Distribution Network Functional Architecture description, Research Centre of Finland, VTT, 2013, pp. 142.

[16] IEC 61850-1, Communication networks and systems for power utility automation - Part 1: Introduction and overview, 1st edition, 2003, pp. 37.

[17] D. Dolezilek, D. Hou, IEC 61850 – What It Can and Cannot Offer to Traditional Protection Schemes, SEL Journal of Reliable Power, Volume 1, Number 2, October 2010, pp 11.

[18] 61850-8-1, Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, 1st edition, 2004, pp. 133.

[19] 61850-9-2 Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3, 1st edition, 2004, pp. 28

[20] S. Borkar, C. Fernandes, J. Gohil, Testing of Goose Protocol of IEC61850 Standard in Protection IED, International Journal of Computer Applications (0975 – 8887), Volume 93, No 16, May 2014, pp. 6.

[21] A. Lemmetyinen, IEC 61850 -standardin soveltaminen sulautetulla Linux-järjestelmällä, Master of Science Thesis, University of Vaasa, 2015, pp. 118, Available: https://www.tritonia.fi/fi/e-opinnaytteet/tiivistelma/6229/IEC+61850+-standardin+soveltaminen+sulautetulla+Linux-j%C3%A4rjestelm%C3%A4ll%C3%A4

[22] IEC 60870-5-104, Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles, Second edition, 2006, pp. 139

[23] T. Littler, K. McLaughlin, B. Pranggono, S. Sezer, H.F. Wang, Y. Yang, Intrusion Detection System for IEC 60870-5-104 Based SCADA Networks, Power and Energy Society General Meeting (PES), Vancouver, BC, Canada, 2013, pp. 5.

[24] Overview of the DNP3 Protocol, DNP Users Group, webpage, Available: http://www.dnp.org/pages/aboutdefault.aspx [Accessed: 1.7.2016]

[25] K. Curtis, A DNP3 Protocol Primer, DNP Users Group, 2005, pp. 8, Available: https://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf [Accessed: 10.7.2016]

[26] R. Amoah, S. Camtepe, E. Foo, Securing DNP3 Broadcast Communications in SCADA Systems, IEEE Transactions on Industrial Informatics, Vol. 12, No. 4, August 2016, pp. 12.

[27] S. Mackay, J. Park, D. Reynders, E. Wright, Modbus overview, Practical Industrial Data Networks: Design, Installation and Troubleshooting, Newnes, 1st edition, 2004, pp.96-114

[28] Introduction to Modbus TCP/IP, Technical Reference – Modbus TCP/IP, ACROMAG INCORPORATED, 2005, pp. 42, Available: https://www.prosoft-technology.com/kb/assets/intro_modbustcp.pdf

[29] MODBUS Messaging on TCP/IP Implementation Guide V1.0b, Modbus Organization, 2006, pp. 46, Available: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf [Accessed: 24.7.2016]

[30] J. Rinaldi, An Overview of EtherNet/IP, An Application Layer Protocol for Industrial Automation, Real Time Automation, 2003, pp. 8, Available: http://rtaautomation.wpengine.netdna-cdn.com/wp-content/uploads/2014/07/EIP_Overview1.pdf [Accessed: 19.7.2016]

[31] The Common Industrial Protocol, Open DeviceNet Vendor Association, Webpage, Available: https://www.odva.org/Technology-Standards/Common-Industrial-Protocol-CIP/Overview [Accessed: 19.7.2016]

[32] A Guide for EtherNet/IP Developers, EtherNet/IP Quick Start for Vendors Handbook, Open DeviceNet Vendor Association, 2008, pp. 41, Available: https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00213R0_EtherNetIP_Developers_Guide.pdf

[33] PROFINET Security Guideline, Guideline for PROFINET, PROFIBUS - PROFINET, Version 2.0, 2013, pp. 47, Available: http://www.profibus.com/nc/download/specifications-standards/downloads/profinet-security-guideline/display/

[34] PROFINET System Description - Technology and Application, PROFIBUS - PROFINET, 2014, pp. 28 , Available: http://www.profibus.com/nc/download/technical-descriptions-books/downloads/profinet-technology-and-application-system-description/display/

[35] PROFInet Unplugged – An introduction to PROFInet CBA, PROFINET CBA, RTA Automation, Webpage, Available: http://www.rtaautomation.com/technologies/profinet-cba/ [Accessed: 5.8.2016]

[36] I. Goyret, J. Lau, M. Townsley, RFC 3931, Layer Two Tunneling Protocol - Version 3 (L2TPv3), The Internet Society, 2005, pp. 94, Available: https://tools.ietf.org/html/rfc3931

[37] Layer 2 Tunnel Protocol Version 3, Cisco, Webpage, Updated: September 13, 2004, Available: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/l2tpv30s.html [Accessed: 1.9.2016]

[38] S. Bryant, P. Pate, RFC 3985, Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture, The Internet Society, 2005, pp. 42, Available: https://tools.ietf.org/html/rfc3985

[39] R. Aggarwal, M. Dos Santos, M. Townsley, RFC 4719, Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3), The Internet Engineering Task Force Trust, 2006, pp. 14, Available: https://tools.ietf.org/html/rfc4719

[40] V. Jain, RFC 4951, Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover", The Internet Engineering Task Force Trust, 2007, pp. 26, Available: https://tools.ietf.org/html/rfc4951

[41] C. Pignataro, T. Nadeau, RFC 5885, Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV), The Internet Engineering Task Force Trust, 2010, pp. 14, Available: https://tools.ietf.org/html/rfc5885

[42] T. Mehmet, Networks and Services: Carrier Ethernet, PBT, MPLS-TP, and VPLS, Wiley, 2012, pp. 432

[43] N. El-Aawar, G. Heron, L. Martini, E. Rosen, RFC 4448, Encapsulation Methods for Transport of Ethernet over MPLS Networks, The Internet Society, 2006, pp. 24, Available: https://tools.ietf.org/html/rfc4448

[44] N. El-Aawar, G. Heron, L. Martini, E. Rosen, T. Smith, RFC 4447, Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP), The Internet Society, 2006, pp. 24, Available: https://tools.ietf.org/html/rfc4447

[45] J. Moy, RFC 2328, OSPF Version 2, The Internet Society, 1998, pp. 244, Available: https://tools.ietf.org/html/rfc2328

[46] D. Farinacci, S. Hanks, T. Li, D. Meyer, P. Traina, RFC 1701, Generic Routing Encapsulation (GRE), 1994, pp. 8, Available: https://tools.ietf.org/html/rfc1701

[47] D. Farinacci, S. Hanks, T. Li, D. Meyer, P. Traina, RFC 2784, Generic Routing Encapsulation (GRE), The Internet Society, 2000, pp. 9, Available: https://tools.ietf.org/html/rfc2784

[48] Z. Xu, Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services: An Advanced Guide for VPLS and VLL, Wiley, 2010, pp. 984

[49] Unencapsulated MS-CHAP v2 Authentication Could Allow Information Disclosure, Microsoft Security Advisory 2743314, Microsoft TechNet , Webpage, Available: https://technet.microsoft.com/library/security/2743314 [Accessed: 15.1.2017]

[50] VPN Tunneling Protocols, Microsoft TechNet, Webpage, Available: https://technet.microsoft.com/fi-fi/library/dd469817(v=ws.10).aspx [Accessed: 15.1.2017]

[51] M. Masoumi, M. Othman, Co-spanning tree restoration mechanism for metro Ethernet switched networks, Photonic Network Communications, Volume 29, Issue 1, February 2015, pp. 118–131

[52] D. Katz, D. Ward, RFC 5880, Bidirectional Forwarding Detection (BFD), The Internet Engineering Task Force Trust, 2010, pp. 49, Available: https://tools.ietf.org/html/rfc5880

[53] M. Bhatia, M. Binderberger, S. Boutros, M. Chen, J. Haas, RFC 7130, Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces, The Internet Engineering Task Force Trust, 2014, pp. 11, Available: https://tools.ietf.org/html/rfc7130

[54] IEEE Standard for Local and metropolitan area networks—Link Aggregation, IEEE Standard, IEEE Computer Society, 2008, pp. 163

[55] C. Pignataro, T. Nadeau, RFC 5085, Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires, The Internet Engineering Task Force Trust, 2007, pp. 30, Available: https://tools.ietf.org/html/rfc5085

[56] J. Á. Araujo, J. Lázaro, A. Astarloa, A. Zuloaga, J. I. Gárate, PRP and HSR for High Availability Networks in Power Utility Automation: A Method for Redundant Frames Discarding, IEEE Transactions on Smart Grid, Volume 6, Issue 5, September 2015, pp. 2325 - 2332

[57] M. Rentschler, H. Heine, The Parallel Redundancy Protocol for industrial IP networks, Industrial Technology (ICIT), 2013 IEEE International Conference, April 2013, Cape Town, South Africa, pp. 6

[58] N.R. Indukuri, Layer 2 Security for Smart grid Networks, IEEE International Conference on Advanced Networks and Telecommunciations Systems (ANTS), Bangalore, India, 2012, pp. 6

[59] IEEE Standard for Local and metropolitan area networks— Media Access Control (MAC) Security, IEEE Standard, IEEE Computer Society, 2006, pp. 142

[60] A. Astarloa, J.A. Araujo, U. Bidarte, J. Lázaro, N. Moreira, MACsec Layer 2 Security in HSR Rings in Substation Automation Systems, Energies 2017, Volume 10, Issue 2, Published 31 January 2017, pp. 15

[61] S. Frankel, S. Krishnan, RFC 6071, IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, The Internet Engineering Task Force Trust, 2011, pp. 63, Available: https://tools.ietf.org/html/rfc6071

[62] IPsec VPN WAN Design Overview, Cisco Systems, 2007, Available: https://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f22f.pdf [Accessed: 20.1.2017]

[63] M.K.N.M. Sarmin, W. Nakawiro, M.Z.C. Wanik, M.F.M. Siam, Z.F. Hussien, A.A. Ibrahim, A.K.M. Hussin, Coordinated Voltage Control in Distribution Network with Renewable Energy Based Distributed Generation, Engineering, Issue 5, 2013, pp. 208-214

[64] H. Reponen, Coordinated Voltage Control in Real Time Simulations of Distribution Network with Distributed Energy Resources, Master of Science thesis, Tampere University of Technology, 2016, pp. 95, Available: https://dspace.cc.tut.fi/dpub/handle/123456789/24109

[65] S. Repo, IDE4L - Functional testing of low voltage distribution network automation, Tampere University of Technology, Available:

https://webhotel2.tut.fi/units/set/ide4l/Functional%20testing%20of%20low%20voltage%20distribution%20network%20automation.pdf [Accessed: 24.4.2017]

[66] IEEE 1646-2004, IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation, IEEE Standard, 2005, pp. 35

[67] G. Clarke, D. Reynders, Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, 1st Edition, Newnes, 2004, pp. 544

[68] T. Amau, K. Kojima, Y. Saka, Y. Saiki, T. Otani, K. Nishiwaki, M Aoki, H. Ukaia, Next-Generation Distribution Automation System Using IEC 61850 GOOSE and Section Switches with Sensors, Electrical Engineering in Japan, Vol. 195, No. 2, 2016, pp. 21-34

[69] I. Ali, S. Hussain, Control and management of distribution system with integrated DERs via IEC 61850 based communication, Engineering Science and Technology, an International Journal, Karabuk University, 2016, pp. 9

[70] C. Hammond, E.A. Udren, J. Wen, Wide-Area Ethernet Network Configuration for System Protection Messaging, 65th Annual Conference for Protective Relay Engineers, College Station, TX, USA, 17 May, 2012, pp. 20

[71] X. Ge, F. Yang, Q. Han, Distributed networked control systems: A brief overview, Information Sciences, volume 380, February 2017, pp. 117–131

[72] R. A. Gupta, M. Chow, Networked Control System: Overview and Research Trends, IEEE Transactions on Industrial Electronics, volume 57, Issue 7, July 2010, pp. 2527 - 2535

[73] J.A. Kay, J.H. Kreiter, D.C. Mazur, Benefits of IEC 61850 standard for power monitoring and management systems in forest products industries, Pulp and Paper Industry Technical Conference (PPIC), Charlotte, NC, USA, 2013, pp. 7

[74] S. Djiev, Industrial Networks for Communication and Control, Elements of Industrial Automation, 2006, pp. 39, Available: http://anp.tu-sofia.bg/djiev/PDF%20files/Industrial%20Networks.pdf [Accessed: 20.05.2017]

APPENDIX A: LIST OF IEC 61850 STANDARD RELATED DOCUMENTS

IEC 61850-7-410	Hydroelectric Power Plants - Communication for monitoring and control.
IEC 61850-7-420	Communications systems for Distributed Energy Resources (DER) - Logical nodes
IEC 61850-7-500	Use of logical nodes to model functions of a substation Automation system.
IEC 61850-7-510	Use of logical nodes to model functions of a Hydro Power Plant.
IEC 61850-90-1	Use of IEC 61850 for the communication between substations
IEC 61850-90-2	Use of IEC 61850 for the communication between control centres and substations
IEC 61850-90-3	Using IEC 61850 for Condition Monitoring
IEC 61850-90-4	IEC 61850 - Network Engineering Guidelines
IEC 61850-90-5	Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118
IEC 61850-90-6	Use of IEC 61850 for Distribution Feeder Automation System
IEC 61850-90-7	Object Models for Photovoltaic,Storage and other DER inverters
IEC 61850-90-8	Object Models for Electrical Transportation (E-Mobility
IEC 61850-90-9	Object Models for Batteries
IEC 61850-90-10	Object Models for Scheduling
IEC 61850-80-1	Guideline to exchanging information from a CDC-based data model using IEC 60870-5-101 or IEC 60870-5-104
IEC 61400-25	IEC 61850 Adaptation for Wind Turbines
IEC 61400-25-1	Wind turbines - Part 25-1: Communications for monitoring and control of wind power plants - Overall description of principles and models
IEC 61400-25-2	Wind turbines - Part 25-2: Communications for monitoring and control of wind power plants - Information models
IEC 61400-25-3	Wind turbines - Part 25-3: Communications for monitoring and control of wind power plants - Information exchange models
IEC 61400-25-4	Wind turbines - Part 25-4: Communications for monitoring and control of wind power plants

	- Mapping to communication profile - Mapping to SOAP-based web services - Mapping to MMS - Mapping to OPC XML DA - Mapping to IEC 60870-5-104 - Mapping to DNP3
IEC 61400-25-5	Wind turbines - Part 25-5: Communications for monitoring and control of wind power plants - Conformance testing
IEC 61400-25-6	Wind Turbines - Part 25-6: Communications for monitoring and control of wind power plants - Logical node classes and data classes for condition monitoring
IEC 62271-3	Communications for monitoring and control of high-voltage switchgear (published)

Source: http://www.liquisearch.com/iec_61850/related_standards